

PROS LITE

User Manual

Version 2.0.0

Table of Contents

Getting Started	5
Starting PROS Lite	5
Create a Portal	5
Adding a control panel	6
Adding a user	7
Upload users to a controller	8
PROS Lite Manual	9
Operator log in	9
Display options	10
Program options	11
Hardware settings	13
Portals	14
What is a portal?	14
Hardware	15
RS232 to RS485	15
USB to RS485	15
TCP/IP to RS485	15
Add a Serial Portal	16
Add a Network portal	16
Search network portals	17
Configure the CNV-1000	17
Edit a portal	19
Delete a portal	19
Firmware update	20
Control panels	21
Hardware	22
EWS	22
EWSi	22
Add a controller	23
Edit a controller	24
Start/stop pooling	25
Upload configuration to a controller	26
Set controller time	26
Upload users database	26
Firmware update	26
Check firmware version	27
Read controller settings	27
Doors	28
Hardware	29
Electric strike	29
Magnetic lock	29
Door contact sensor	29
Egress button	30
Configuring a door	30
Door control	32
Readers	33
Hardware	34
Proximity readers	34
Fingerprint readers	35

	BioXr	35
	BioIn Prox	35
	BioC	35
	Configuring readers	36
	Fingerprint readers	38
	Add or modify a reader	38
	Check firmware version	40
	Firmware update	40
	Read reader settings	40
	Upload configuration to a reader	40
	Sensor calibration	40
	Inputs	41
	Input configuration	41
	Outputs	43
	Output configuration	43
	Output control	44
	Access settings	45
	Time zones	45
	Holidays	45
	Access levels	47
	Adding Access level	47
	Edit access level	48
	Delete Access Level	48
	Departments	49
	Add a Department	49
	Edit a Department	49
	Delete a Department	49
	Users	50
	Add a user	50
	Edit a user	51
	Delete a user	51
	Fingerprints	53
	Read me first	53
	Enrolling Fingerprints from a reader	53
	Enrollment from a desktop Reader	53
	Uploading the fingerprints to the Fingerprint readers	54
	Deleting Fingerprints	55
	Deleting one user from the fingerprint Reader	55
	Deleting all users from the fingerprint Reader	55
	Deleting user finger templates from the Software	55
	Complex upload	55
	Reports	57
	User list report	57
	Access reports	58
	Load report window	58
	Set time filters	58
	User report	59
	Unknown ID report	59
	Department report	60
	Adding a reader filter to Access report	60
	Adding a Doors filter to Access report	60
	I/O reports	62
	Load report window	62
	Set time and controllers filters	62
	Inputs report	63
	Outputs report	63
	Doors report	63
	HardwareReport	64
	Load report window	64

Set time and controllers filters 64

Program operators 66

Add an operator 66

Edit an operator 66

Delete an operator 66

Troubleshooting 67

Biometry 67

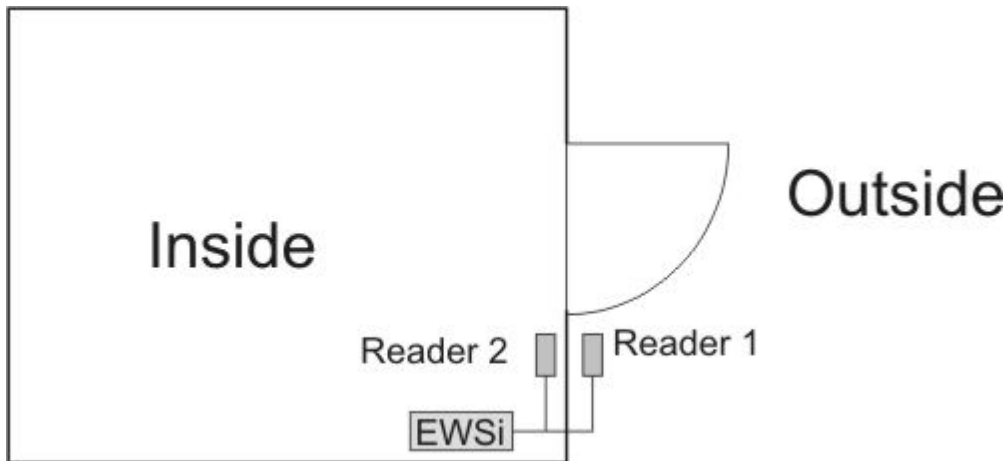
Glossary 69

Getting Started

This Getting Started Guide will use examples to guide you through the minimum configuration required after installing the PROS Lite.

This example assumes that the system contains the following elements:

1. Access controller EWSi (2 Reader controller with a built-in CNV1000 TCP/RS485 network converter), controlling main entry to the building with Reader 1 outside and Reader 2 inside.
2. Both readers should be standard proximity readers with a Wiegand 26 bit interface.



Starting PROS Lite

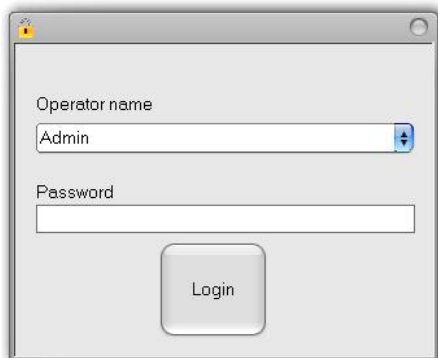
- Run PROS

Select PROS from the **Start>All Programs>XPR>PROS Lite** menu or double-click on the PROS Lite icon on your desktop.



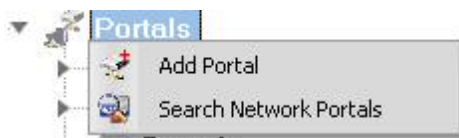
- Login

On the PROS main menu, select **Program>Log in**. On the login window, select operator and enter the password (The default setting is Operator name = "Admin" and "Password = "admin")

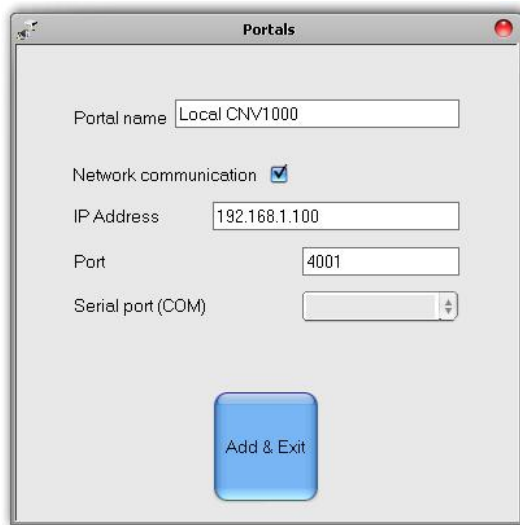


Create a Portal

- Right-click on the **Portals** item and select **Add portal**



- Consult your installer for the portal IP address and Port, and fill in the Portal properties window with the data.



- Click on **Add & Exit**
- The new portal will be shown below the Portals item

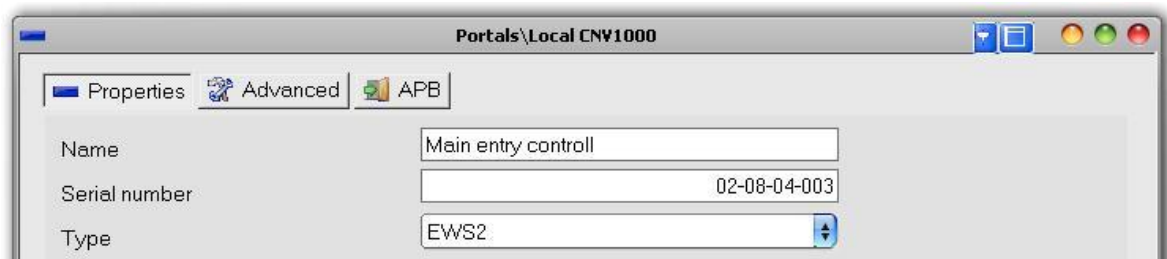


Adding a control panel

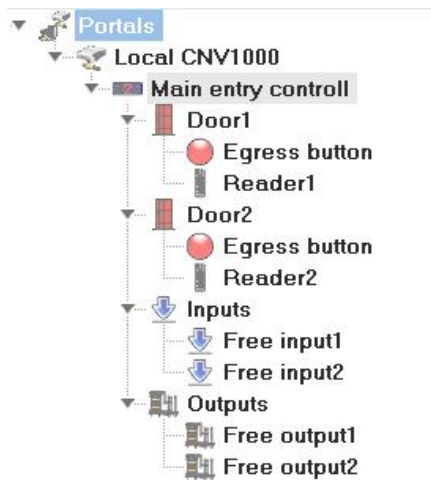
- Right-click on the new portal *Local CNV1000* item and select **Add controller>EWS**



- Consult your installer for the controller Serial number and fill in the controller properties window with the data.



- Click on **Save & Exit** button
- The new controller and controller peripherals are shown under the portal item.

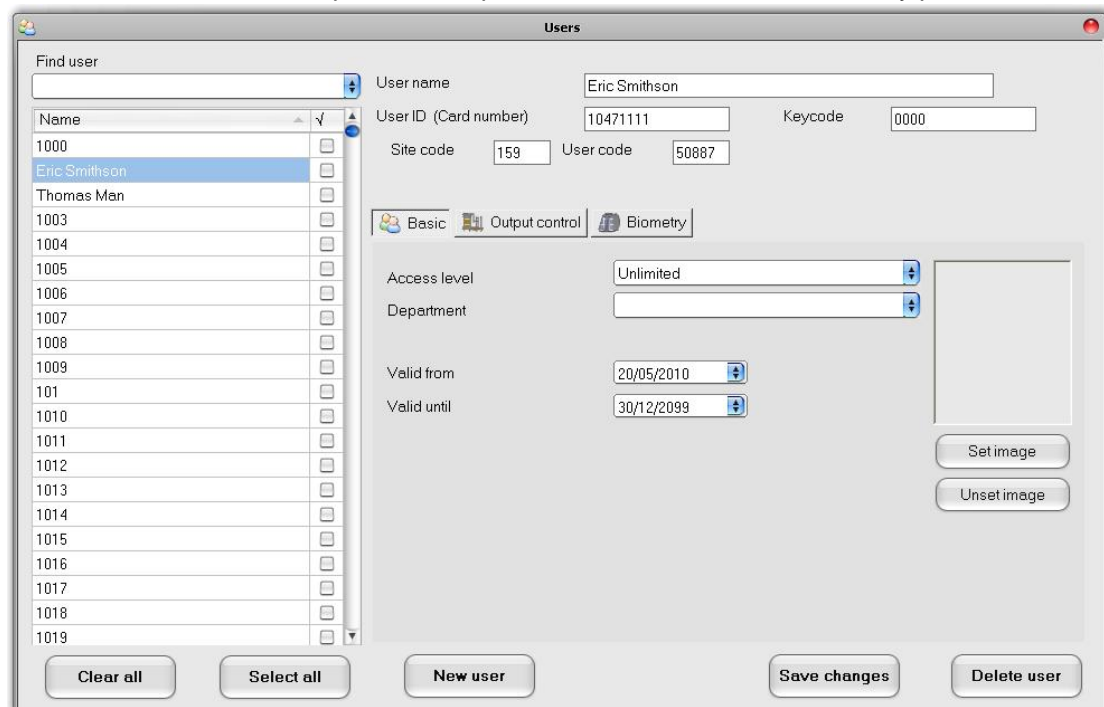


Adding a user

- Double-click on the **Users** item



- On the Users window click on **New user**. The button caption will change to "Save".
- Enter the Name of the user, the user ID (card number), select Unlimited in the Access level drop-down list box, select General in the Department drop-down list box and select the validity period from-until.

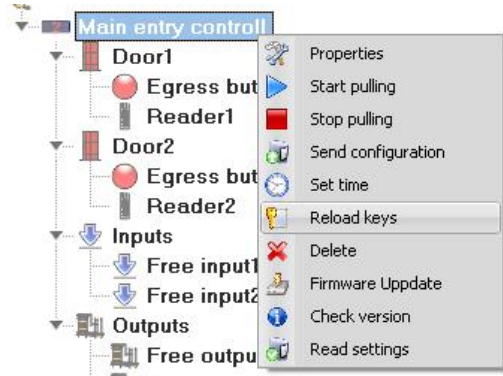


- Click on **Save**
- The entered user will be added to the user table on the left

Name	✓
Tomas M Solace	

Upload users to a controller

- Right-click on controller item and select **Reload keys**



- Information about the controller update will be added to the event table

Time	Portal	Controller	Reader	Door	Event	User	Key	Image
11/04/2010 22:05:11	Local CNV1000	Main entry controll			Load users finished			
11/04/2010 22:05:10	Local CNV1000	Main entry controll			Loading users			
11/04/2010 22:05:10	Local CNV1000	Main entry controll	PREDRAG2	Admin	Clear keys	OK		

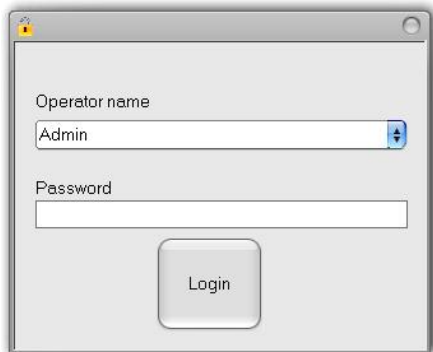
PROS Lite Manual

Operator log in

PROS starts without an operator logged in. Only event pulling will be running. Logging in allows changing operator options.

How to log in:

Select **Program>Log in** in the PROS main menu. On the login window select operator and enter the password. The default password for the user Administrator is "admin".



How to log off:

In the PROS main menu select **Program >Log out**.

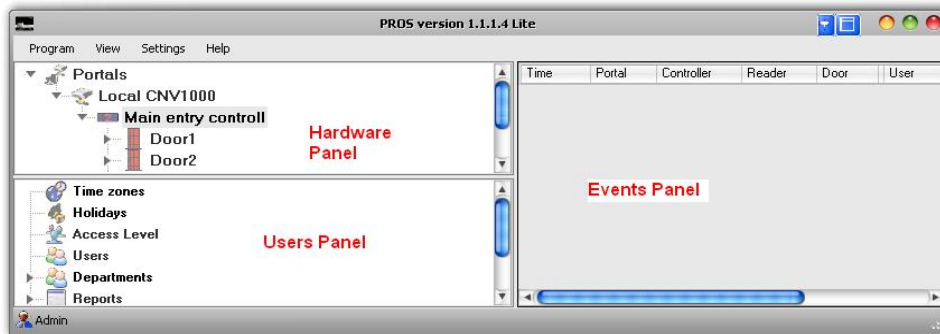
Program options	Operator options					
	Hardware configuration	User management	Operator management	Report view	Program	Access system online control
Main menu						
System parameters					•	
Panels view settings					•	
Upload table		•				
Portals menu						
Add portal	•					
Search portals	•					
Portal menu						
All options	•					
Controller menu						
Modify properties	•					
Start pulling					•	•
Stop pulling					•	•
Configure controller	•					
Set controller time	•					•

Reload keys		•				
Delete controller	•					
Firmware update	•					
Check version online	•					•
Read settings from controller	•					•
Reader menu						
Modify properties	•					
Enable reader	•					
Disable reader	•					
Check version online	•	•			•	•
Firmware update	•					
Read settings from reader	•	•				•
Configure reader	•					
Calibrate sensor	•	•				•
Input menu						
Modify properties	•					
Door menu						
Modify properties	•					
Open door	•					•
Lock door	•					•
Unlock door	•					•
Output menu						
Modify properties	•					
Enable	•					•
Disable	•					•
Activate	•					•
Operators						
All options			•			
Access levels						
All options		•				
Departments						
All options		•				
User management						
All options		•				
Reports						
All options				•		

Display options

Display panels

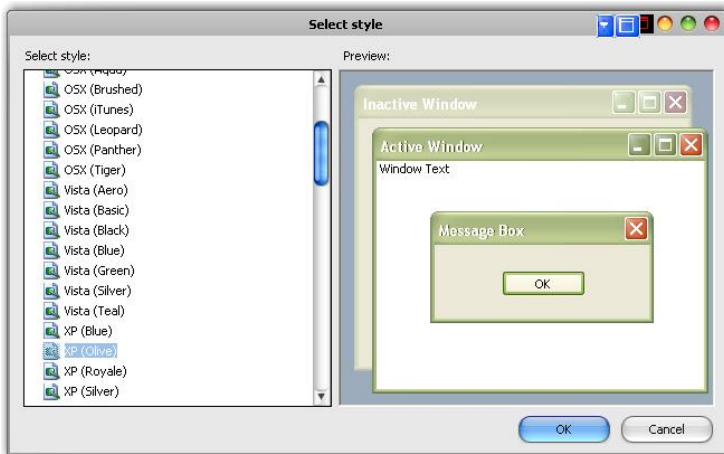
PROS' main area is divided into Hardware management, Users management and Events displaying panels.



Each panel can be hidden or made visible by using options in the **View** menu.

Display style

Visual appearance can be selected from the menu **View>Appearance>Style**



The Style is stored with the operator's properties and is loaded at operator log in.

Shadow style

The shadow style can be selected from the menu **View>Appearance>Shadow style**

Program options

Select **Settings>System parameters** from the main menu



Keycode length: Defines the number of digits used for a keyed-in code, if the installed hardware supports keycode access. This value is valid for all equipment. If entered values for the keycode are longer than the selected value, digits will be removed from left to right. For example, if the keycode was 12345678 and the keycode was reduced to a length of 5 digits, the new keycode sent to the equipment would be 45678. If the length was increased, the necessary number of zero (0) digits would be added to the left side of the keycode so that the required length is achieved. If the keycode has a value of zero (0), it will be considered as "no keycode".

Events display control: The events table contains images that can use up a large amount of system memory and reduce system performance. Therefore when the events table reaches a pre-defined maximum number of events shown, the row number will be reduced to the latest defined number of events.

Auto Logon: If enabled, the selected user will be logged in at program start if the correct password is entered.

Automatic update options:

- If this Controller's option is checked, the controllers will be updated when any changes are made by PROS. For example, if the Controller properties form is open, a click on the "Save & Exit" button will invoke the update procedure and send the new settings to the controller. If the update is not possible (controller is not on-line, not mounted yet, network malfunctioning ...), the event will be added to the event panel and must be performed manually later.

- If the Users option is checked, for every Save command on forms containing relevant user configuration, user data will be sent to all the controllers in the system. If some of the controllers do not respond, the event will added to the event panel.

- If the Date & Time option is checked, PROS will update the controller's date and time on start and every 12 hours if already running.

- If the Biometry option is checked, the biometric devices will be updated when the properties form is closed with the "Save" button.

Hardware settings

Portals

What is a portal?

A Portal is a communication link between PROS and the devices in the system. A Portal has two parts - logical, recognizable by the software, and physically – an electronic device connected to a computer and other devices in the system known as converters.

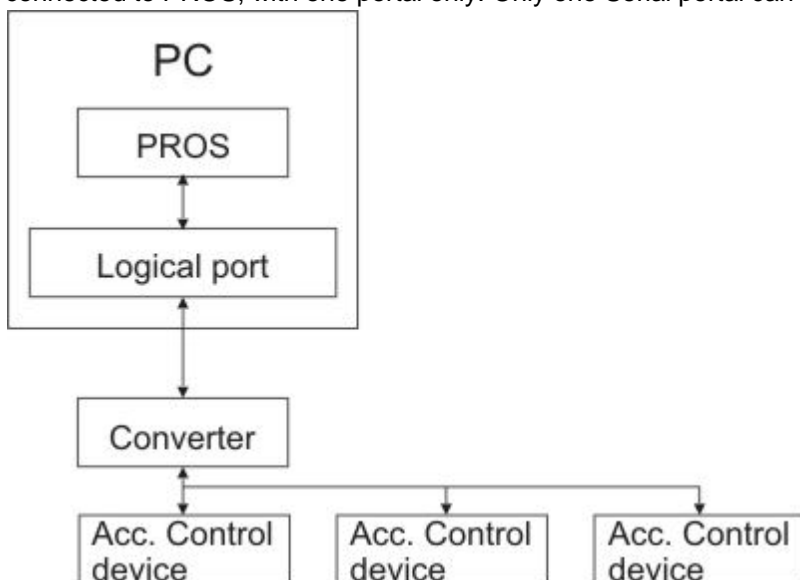
The Logical part can be:

1. Serial port (COM)
2. Network port

The Physical part can be:

1. RS232 to RS485 converter, connected to a logical Serial port
2. USB to RS485 converter, connected to a logical Serial port
3. TCP/IP to RS485 converter, connected to a logical Network port

PROS can use more than one portal to connect to devices in the system. Devices in the system can be connected to PROS, with one portal only. Only one Serial portal can be used in PROS.



Hardware

RS232 to RS485

This converter is connected to the PC's COM port. It is powered by the COM port so it does not require a separate power supply, except in the case that the PC's COM port does not have all its signal outputs used for power (DTR, RTS) or enough power to drive the converter. This converter does not require any drivers to be installed if the COM port on the PC side is installed properly.

Requirements:

- Available PC COM port (RS232)



CNV-100 RS232 to RS485 converter

USB to RS485

This converter is connected to the PC's USB port. It is powered by the USB port so it does not require a separate power supply, except in the case that the PC's USB port does not have enough power to drive a converter. This converter needs the suitable driver to be installed before use. If installed using the PC's driver manager it will appear as a COM port.

Requirements:

- Available PC USB port
- Device driver



CNV-200 USB to RS485 converter

TCP/IP to RS485

This converter is connected to the PC over a local network or directly with a network patch cable. It uses an external power supply. This converter does not need any drivers to be installed. Some Access control

equipment may have a built-in TCP converter used by the same device and other devices in the system to communicate with PROS.

Requirements:

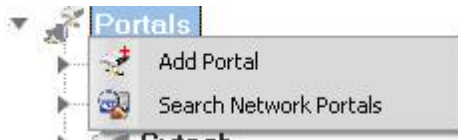
- Access to local network or PC network card.



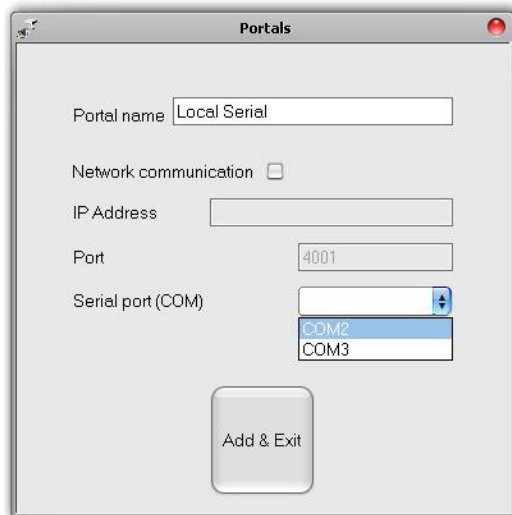
CNV-300 TCP/IP to RS485 converter

Add a Serial Portal

- Right-click on the **Portals** item and select "Add portal"



- Enter the portal name
- Make sure that the Network communication option is not checked
- Select the COM port from the Serial port drop-down list

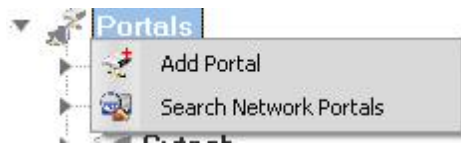


- Click on **Add & Exit**
- The New portal is shown below the Portals item with a given name and a picture of the serial portal

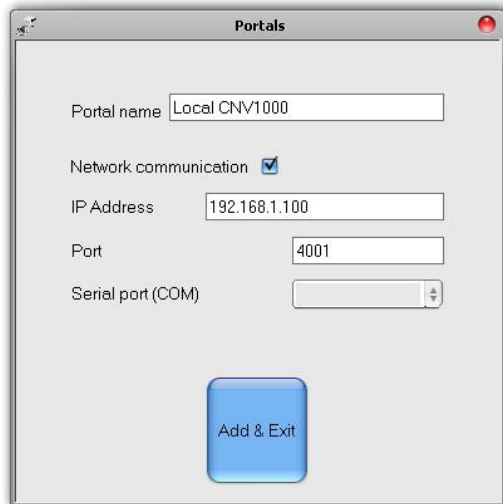


Add a Network portal

- Right-click on the **Portals** item and select "Add portal"



- Check the Network communication option
- Consult your installer for the portal's IP address and Port, and fill in the Portal properties window with the data.



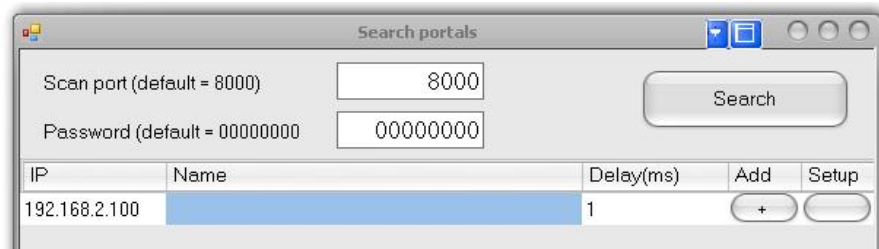
- Click on **Add & Exit**
- The new portal is shown below the Portals item with a given name and a picture of the network portal



Search network portals

This procedure is valid only if you have a CNV1000 TCP convertor device with built-in CNV1000

- Right-click on the Portals icon and select the Search network portals
- On the Search portal window select the port to search (default is 8000)
- Click on the Search button and wait
- If any portal is found, it will be displayed in the table



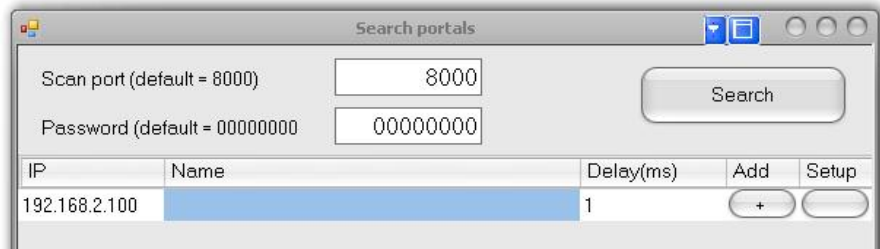
- If the Portal does not exist in PROS, click on the Add column button in the portal row.
- The Portal will be added to your collection of Portals with the same name as the found device IP



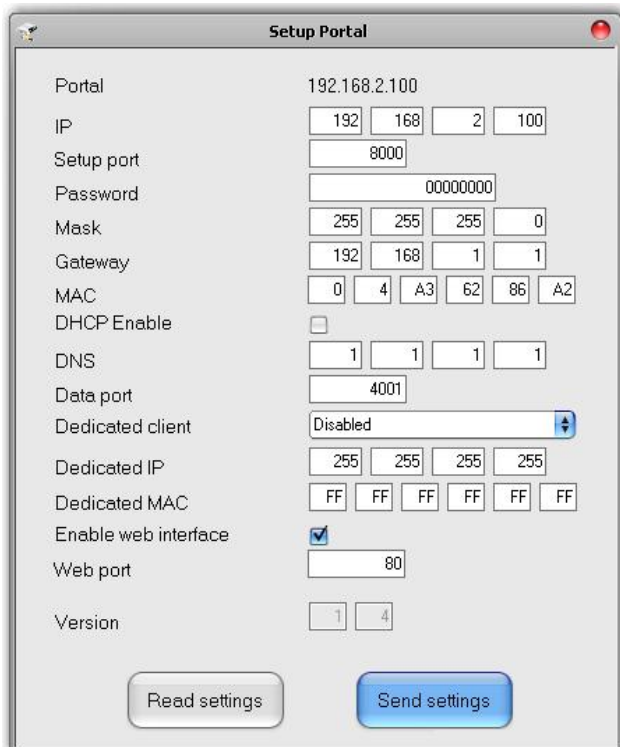
Configure the CNV-1000

- Right-click on the Portals icon and select the Search network portals

- On the Search portal window select the port to search (the default is 8000)
- Click on the Search button and wait
- If any portal is found, it will be displayed in the table



- Enter an 8 digit device password (factory default is 00000000)
- Find a row with a portal to configure and click on the appropriate Setup button
- The setup portal window is shown with the portal settings. If the values are empty, reading settings from CNV-1000 will not be possible



- Enter new settings:
 - **IP:** IP address of device
 - **Setup port:** Network port for search and setup. Changing is not recommended
 - **Password:** Password for access to read and change the settings of the CNV-1000. It is recommended to change the default password and use it for all converters in the system.
 - **Mask:** Enter the device subnet mask
 - **Gateway:** Default gateway
 - **MAC:** Physical address of the device. Changing is not recommended
 - **DHCP Enable:** Enable the DHCP client
 - **DNS:** Address of the DNS server
 - **Data port:** Port used for communication between PROS and devices behind the converter
 - **Dedicated client:** To forbid unauthorized access to devices connected to the portal from another system, select one of the following options
 - Disabled** - no source security checking
 - MAC only** - the source MAC address must be equal to the Dedicated MAC value
 - IP only** - the source IP address must be equal to the Dedicated IP value
 - IP or MAC** - at least one of the conditions from point b and c must be true
 - IP and MAC** - both b and c conditions must be true

- **Enable web interface:** enable or disable the CNV-1000 web interface for configuration
- **Web port:** Web interface port
- **Version:** Read-only field displaying the firmware version of the converter
- Click on Send settings to configure the device, wait for the result message

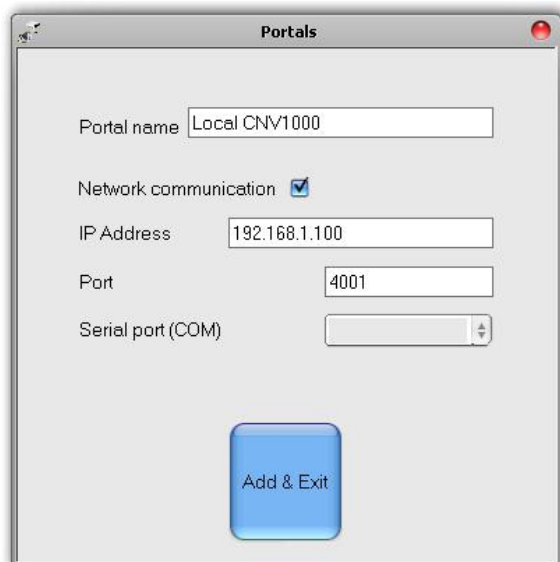


Edit a portal

- Right-click on portal and select Properties



- Change the settings on the properties window



- Click on the Save & Exit button

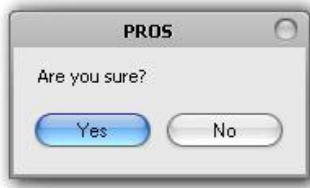
Delete a portal

The Portal can be deleted only if there is no device added to it

- Right-click on the portal and select the Delete menu



- Confirm deletion



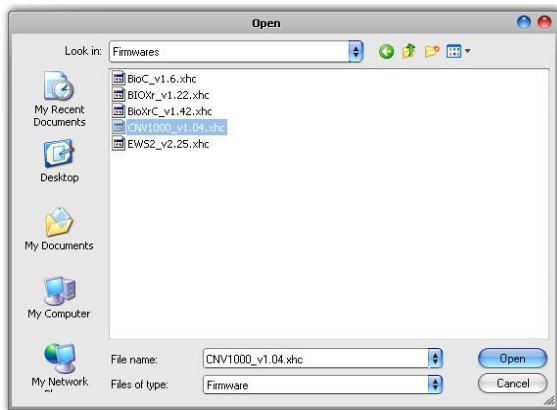
Firmware update

A Firmware update can only be done to a CNV-1000 standalone or embedded converter

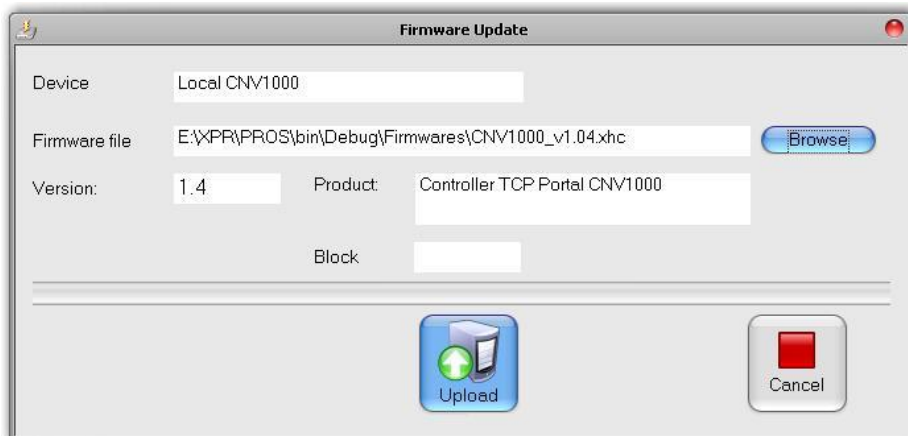
- Check the portal firmware version by using the [Configure CNV-1000](#) procedure
- Right-click on the portal to be updated and select the Firmware update menu



- On the Firmware update window, click the Browse button. The default location of the firmware files installed with PROS is in the PROS folder under "Firmware" folder. If you have a newer version, use browse to locate it.



- Select the firmware file with a ".xhc" extension
- Check the firmware version. If the version is not greater than the existing version of the CNV-1000 then do not upgrade with this file, unless specified by the installer or manufacturer of this device.



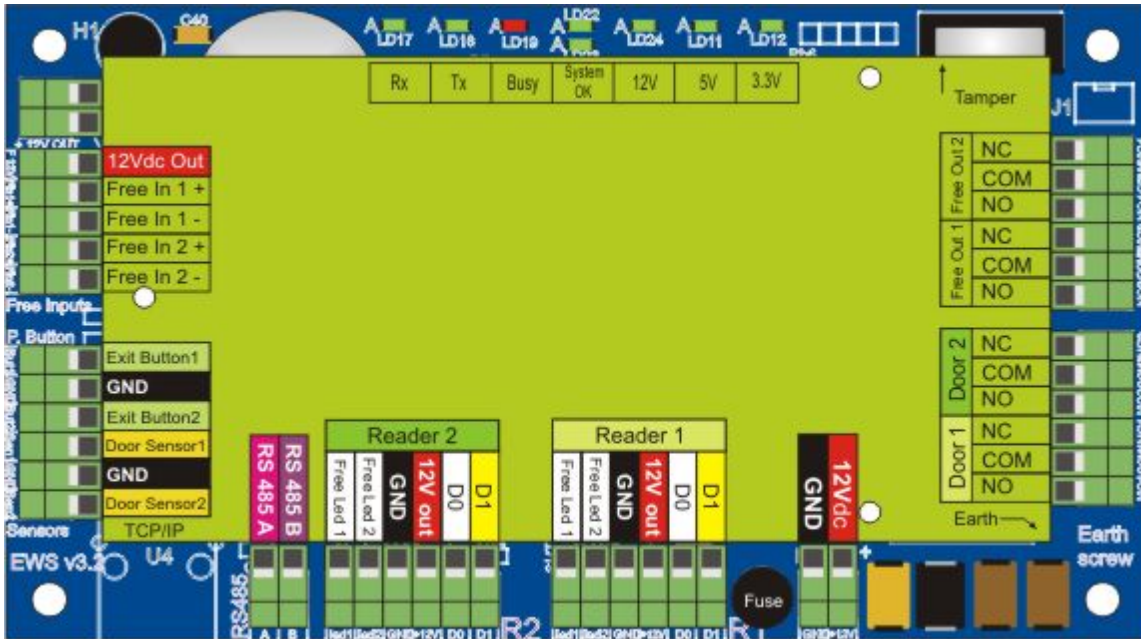
- Click on the Upload button
- Wait for the "Update End Message"
- Close the Firmware update window

Control panels

Hardware

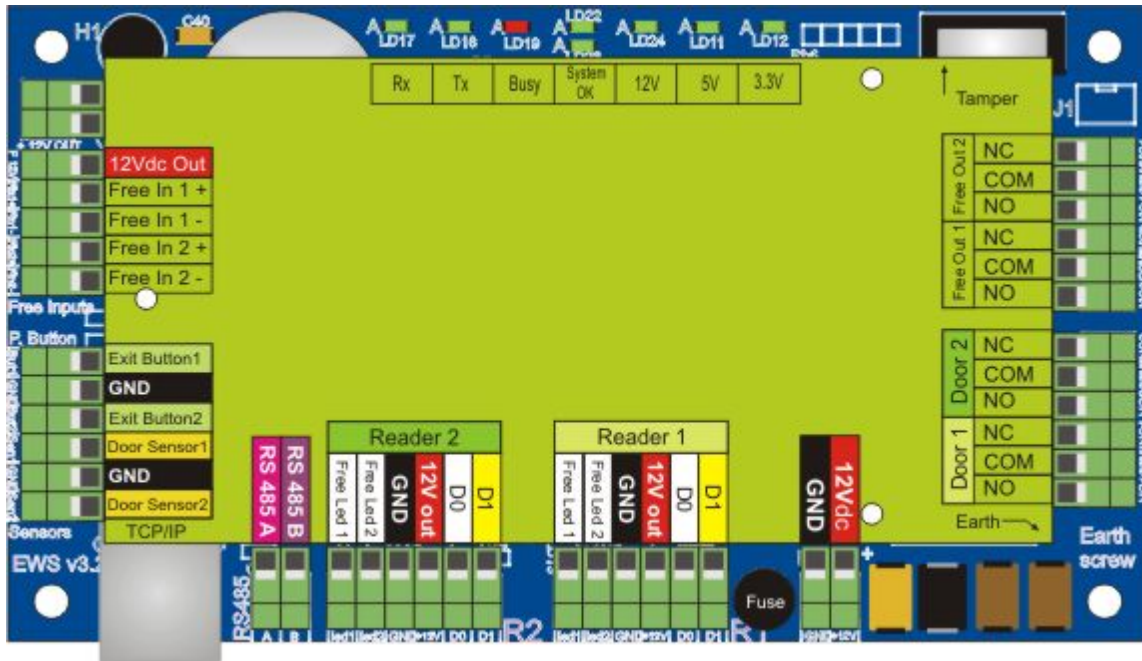
EWS

EWS is an Access control panel with the ability to control up to 2 doors, 2 readers, 2 door contacts, 2 door locks, 2 inputs and 2 outputs (relays). Communication with PROS is through the RS485 interface.



EWSi

EWSi is an Access control panel with the ability to control up to 2 doors, 2 readers, 2 door contacts, 2 door locks, 2 inputs and 2 outputs (relays). With a built-in CNV-1000 TCP to RS485 converter, communication with PROS can be through either Ethernet or RS485. Also, if connected to an Ethernet, other readers and controllers can be reached by PROS if they are connected to the RS485 port of EWSi.

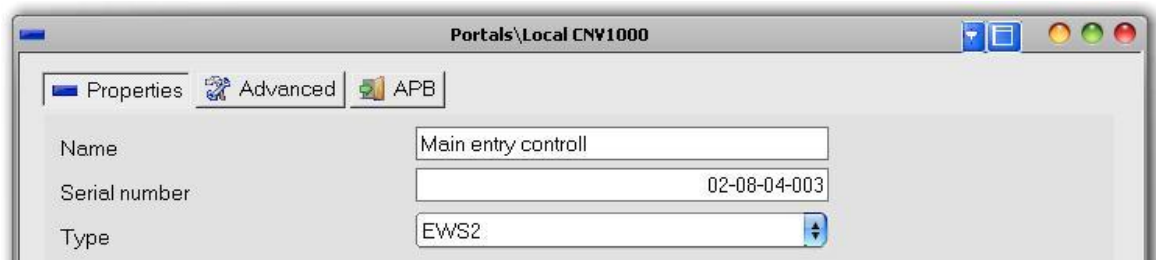


Add a controller

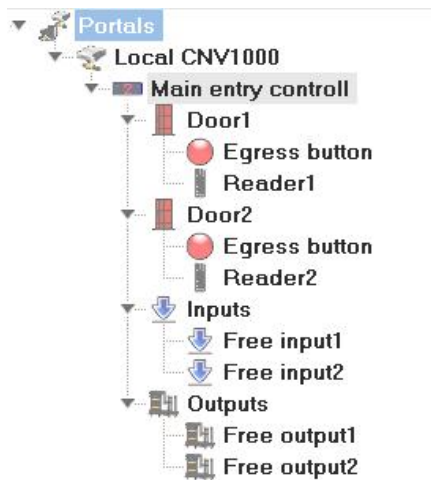
- Right-click on a portal connected to the controller and select **Add controller>EWS**



- Enter Name and Serial number of the controller. The Serial number is provided on the controller's board.



- Click on the Save and Exit button
- The New controller and the controller peripherals are shown under the portal item



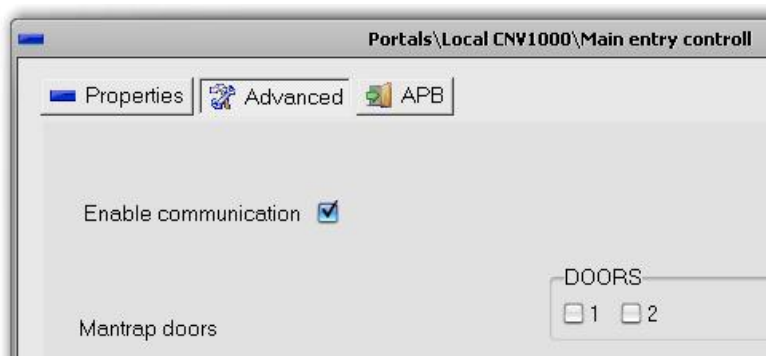
- In order to see if EWS is online and communicating with the PC, right click on the Controller and select “Check Version” from the controller drop-down menu. In the event panel it will be indicated if the controller is on line or not. If the Serial Number does not match, the controller will not go on line. If there is no communication, the controller name will have a red background color in the tree view.

Edit a controller

- Right-click on the controller and select the Properties menu



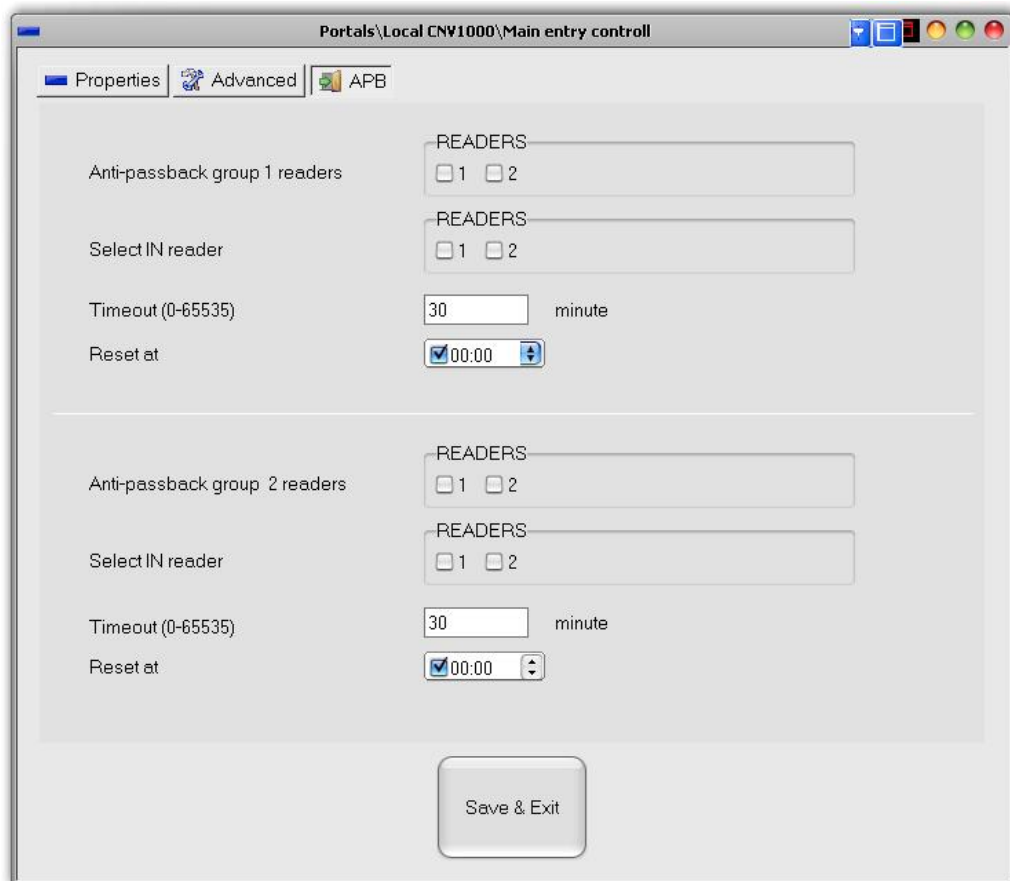
- On the controller properties window select the Advanced tab



- **Enable communication:** When PROS is started, the event pooling from the controller will not run until it is started manually via the controller menu option "Start pooling"

- **Mantrap doors:** If the mantrap option is used, check the doors to be used in the mantrap

- Select APB tab (anti-passback)



- Configure two Anti-passback reader groups if required
 - **Anti-passback group readers:** select the readers in the APB group
 - **Select IN reader:** Select the readers allowing entry to the protected area in the APB group. The selected readers must also be selected in the Anti-passback group readers.
 - **Timeout:** Set the time period, in minutes, required to allow the user to enter the protected area again without exiting the same area. If this option is not required, enter 0.
 - **Reset at:** The time of the day for the APB options to be reset. All users will be considered as out of the protected area.
- Click on the Save & Exit button.
- If the Automatic update for controller's option is set, PROS will configure the controller immediately. If it is not set, update the controller manually via the controller menu option "Send configuration"



Start/stop pooling

- Right-click on the controller and select the Start or Stop pooling menu



This setting will be valid until PROS is closed.

Upload configuration to a controller

- Right-click on the controller and select the Send configuration menu



- See the events panel to check the configuration flow

Set controller time

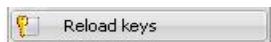
- Right-click on the controller and select the Set time menu



The Time and Date value from the PC will be sent to the controller. Check the PC's time and date accuracy before using this command.

Upload users database

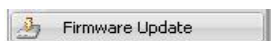
- Right-click on the controller and select the Reload keys menu



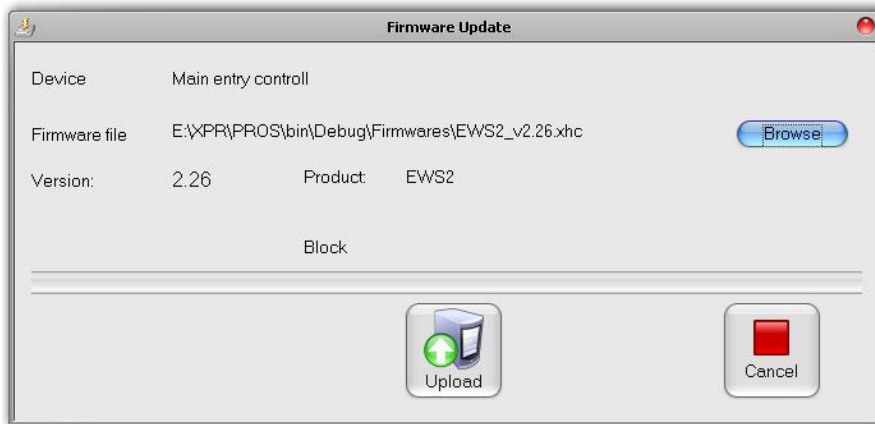
This command will erase the controller user database and upload users from the PC database

Firmware update

- Check the controller firmware version
- Right-click on the controller and select the Firmware update menu



- On the Firmware update window, click the Browse button. The default location of the firmware files installed with PROS is in the PROS folder under "Firmware" folder. If you have a newer version, use browse to locate it.
- Select the firmware file with an ".xhc" extension.
- Check the firmware version. If the version is not greater than the existing version of the controller then do not upgrade with this file unless specified by the installer or manufacturer of this device.



- Click on the Upload button
- Wait for the "Update End Message"
- Close the Firmware update window

Check firmware version

- Right-click on the controller and select the Check version menu



The version is displayed in the events panel

Read controller settings

- Right-click on the controller and select the Check version menu



This option should only be used for a customer support diagnostic

Doors

Hardware

Electric strike

There are many manufacturers of strikes, and there are many things that have to be considered when buying one, i.e. type of jamb, type of locking hardware, whether you require fail secure or fail safe, length of latch, depth of jamb, voltage requirements and the length of the faceplate. In some cases it is better to go with a Magnetic lock.



Sample picture.

Magnetic lock

A magnetic lock is a simple locking device that consists of an electromagnet and armature plate.



Sample picture.

Door contact sensor

The sensors are standard magnetic door sensors used in security applications. Either Normally Open or Normally Closed Sensors can be used. Normally Closed sensors (door closed, switch closed) are recommended so that an alarm can be generated if the connection wire breaks.



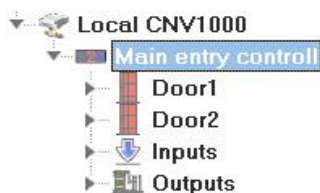
Egress button

Can be either a mechanical push-button or an electronic touch sensor.



Configuring a door

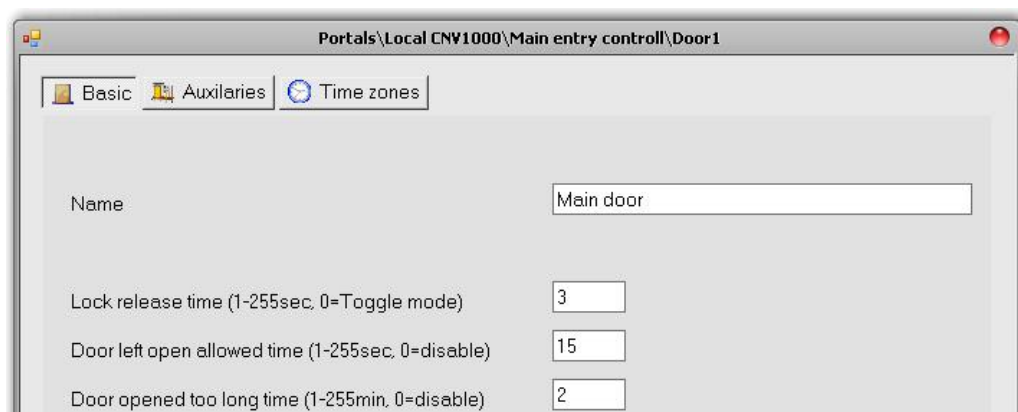
- Expand the controller item to see the doors



- Right-click on the door to be configured and select the Properties item from the door drop-down menu



- Set the values in the Door Basic tab



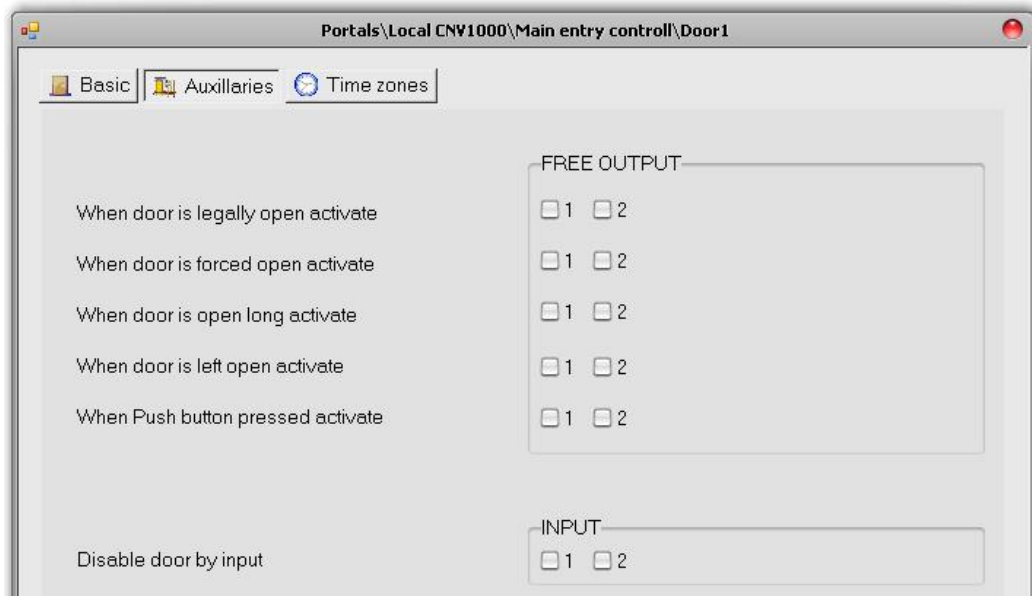
- **Name:** Enter Door Name

- **Lock release time:** The lock release time can have a value between 1 to 255 seconds. If toggle operation is needed, enter 0.

- **Door left open allowed time:** The time allowed for the door to be left open after authorized access and before the Door open too long event (alarm) is invoked. If there is no limit, enter 0.

- **Door opened too long time:** The time allowed for the door to be open after authorized access and before the Door open too long event (alarm) is invoked. If there is no limit, enter 0.

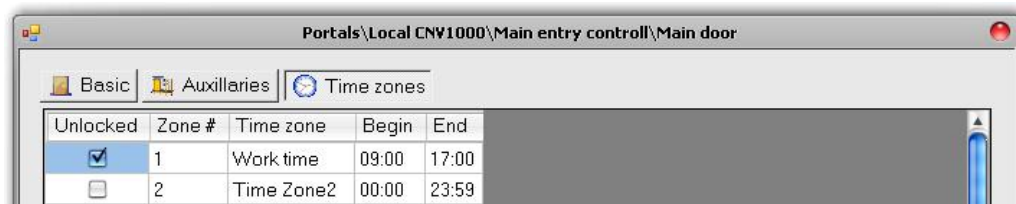
- Set the values in the Auxiliaries tab



- **OUTPUTS:** Select the door event(s) that will activate the relay outputs (except door relays; door relays follow the authorization rule)

- **INPUTS:** Select if any input should disable the door

- Select the Time zones tab and check the time zones during which the door lock should be released



- Click on the Save & Exit button
- Repeat the door configuration procedure on the other doors driven by the same controller
- If the Automatic update for controllers option is set, PROS will configure the controller immediately, if it is not set, update the controller manually with the controller menu option "Send configuration"



Door control

- Right-click on the door to control and select the control item from the door drop-down menu



- **Open:** Acts as legal access to the door, door behavior is the same as normal access
- **Lock:** Locks the door so that it can't be opened by users
- **Unlock:** Cancels the Lock command

Readers

Hardware

Proximity readers

PROS lite supports readers with 26 and 34 bit output.



Metal prox reader with a Wiegand output

Fingerprint readers

BioXr

Fingerprint reader with keypad. Can be set to 26, 34 or custom Wiegand output. Authentication modes can be Finger, Finger and Keycode and Finger or Keycode.



BioIn Prox

Wall mount Fingerprint with Proximity reader.



BioC

Fingerprint reader with a Wiegand output



Configuring readers

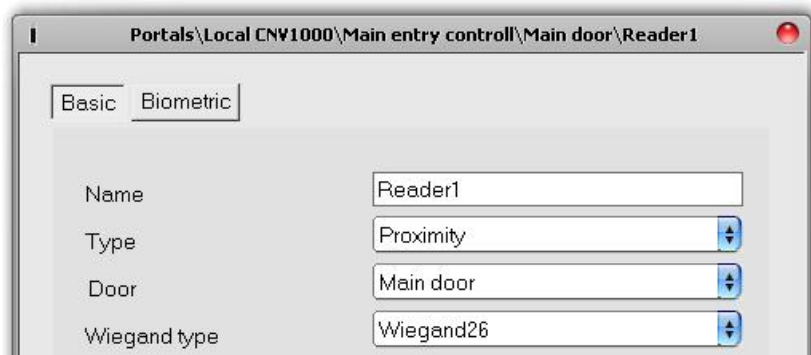
- Expand the Door item to view the readers



- Right-click on the reader to be configured and select the Properties item from the reader drop-down menu



- Set the values in the Basic tab



Portals\Local CNV1000\Main entry controll\Main door\Reader1	
Basic Biometric	
Name	Reader1
Type	Proximity
Door	Main door
Wiegand type	Wiegand26

- **Name:** Enter the Reader's Name
- **Type:** Select the Reader's Type
- **Door:** Select which controller door the reader is attached to
- **Wiegand type:** Select the Wiegand type of the Reader

- Click on the Save & Exit button
- Repeat the reader configuration procedure on the other readers driven by the same controller
- If the Automatic update for controllers option is set, PROS will configure the controller immediately, if it is not set, update the controller manually using the controller menu option "Send configuration"



Fingerprint readers

If fingerprint readers are used, additional reader menu items are available

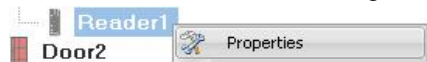


Add or modify a reader

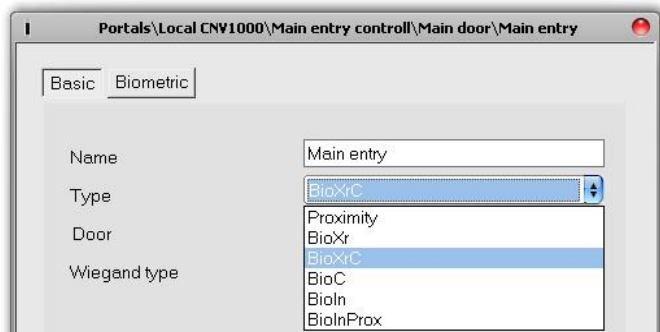
- Expand the Door item to view the readers



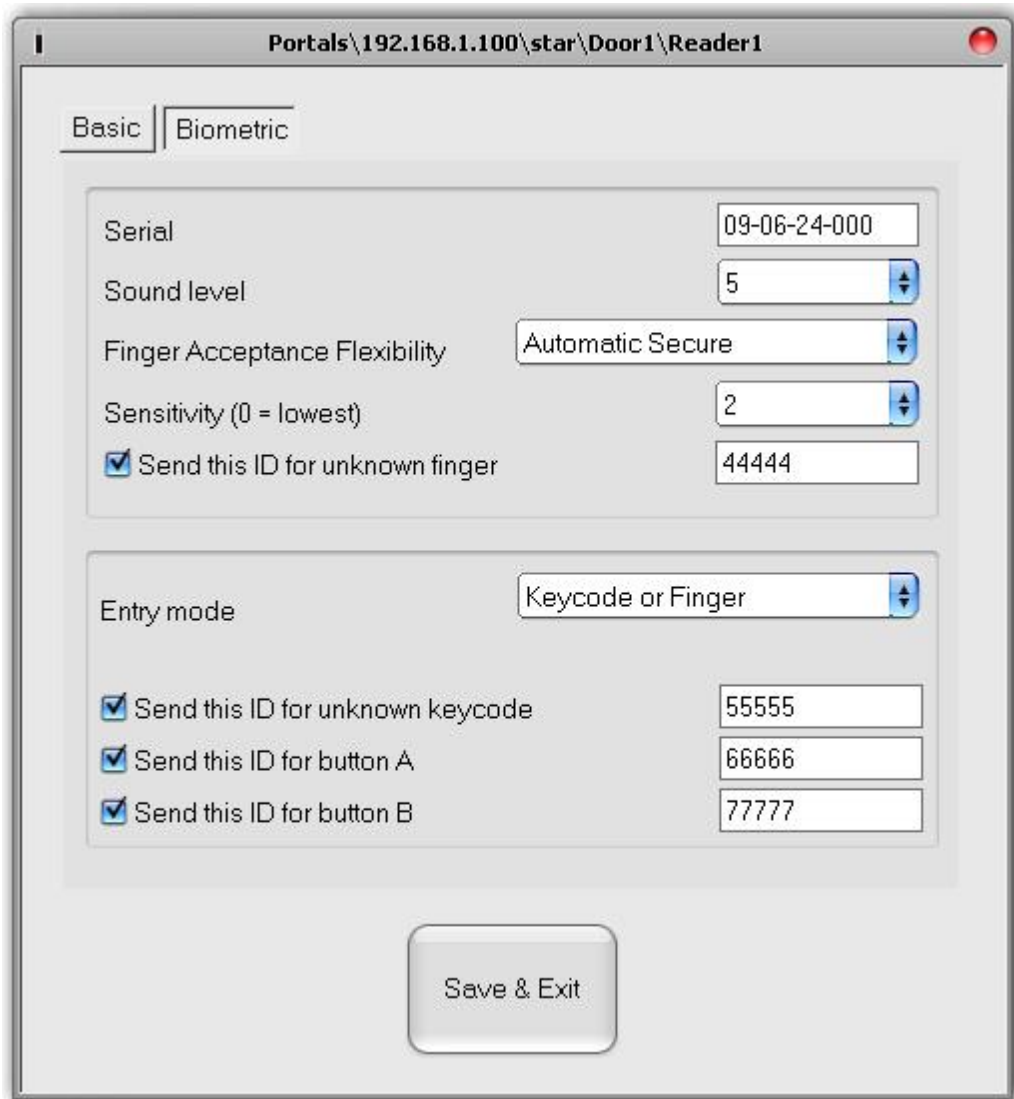
- Right-click on the reader to be configured and select the Properties item from the reader drop-down menu



- Set the reader type to one of the fingerprint models in the Basic tab



- Select the Biometric tab and set the values



- **Serial:** Fingerprint Reader Serial Number

- **Sound level:** Sound level of the device

- **Finger Acceptance Flexibility:** Accepted tolerance. The recommended value is "Automatic Secure".

- **Sensitivity:** Bio-sensor sensitivity, the recommended value is 7, most sensitive.

- If devices have a keypad (BioXr, BioXrC), further settings will be available:

- **Entry mode:**

"**Finger**" (the keypad is inactive)

"**Finger or keypad**" (The Fingerprint Reader will be configured to accept either PIN Codes or fingers)

"**Finger and Keypad**" (The Fingerprint Reader will be configured for double security, requiring a PIN Code and a corresponding finger. Only the right combination will send the user Wiegand to EWS)

- **Send This ID for:**

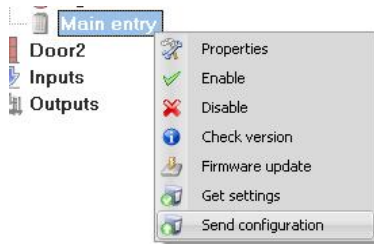
Unknown Finger sends the desired Wiegand when an unknown finger is applied.

Unknown PIN sends the desired Wiegand when an unknown Pin Code is applied.

Button "A" Pressed sends the desired Wiegand when button "A" is pressed.

Button "B" Pressed sends the desired Wiegand when button "B" is pressed.

- Click on the Save & Exit button
- If the Automatic update for biometry option is set, PROS will configure the reader immediately, if it is not set, update the reader manually using the reader menu option "Send configuration"



Check firmware version

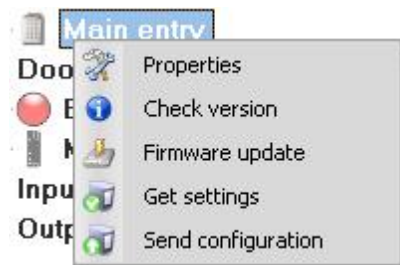
- Right-click on the reader and select the Check version item

Firmware update

- Check the reader firmware version
- Right-click on the reader and select Firmware update menu
- On the Firmware update window, click on the Browse button. The default location of the firmware files installed with PROS is in the PROS folder under "Firmware" folder. If you have a newer version, use browse to locate it.
- Select the firmware file with a ".xhc" extension
- Check the firmware version. If the version is not greater than the existing version of the reader then do not upgrade with this file unless specified by the Installer or manufacturer of the device.
- Click on the Upload button
- Wait for the update end message
- Close the Firmware update window

Read reader settings

- Right-click on the reader and select the Get settings menu



Upload configuration to a reader

- Right-click on the reader and select the Send configuration menu
- See the events panel to check the configuration flow

Sensor calibration

- Right-click on the reader and select the Calibrate menu
- See the events panel to check the Calibration flow

It is recommended to perform a sensor calibration once the reader has been mounted. Clean the fingerprint sensor before calibration.

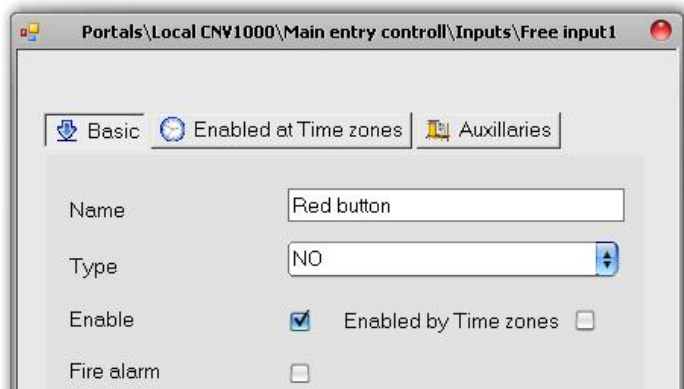
Inputs

Input configuration

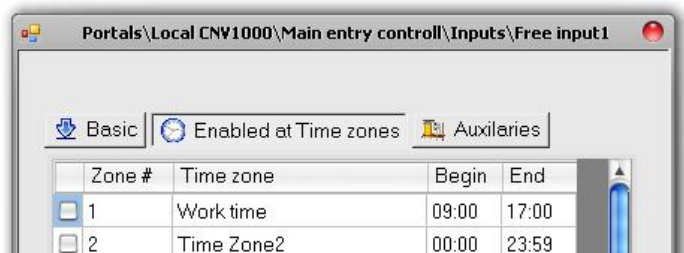
- Right-click on the input to configure and select the Properties item from the input drop-down menu



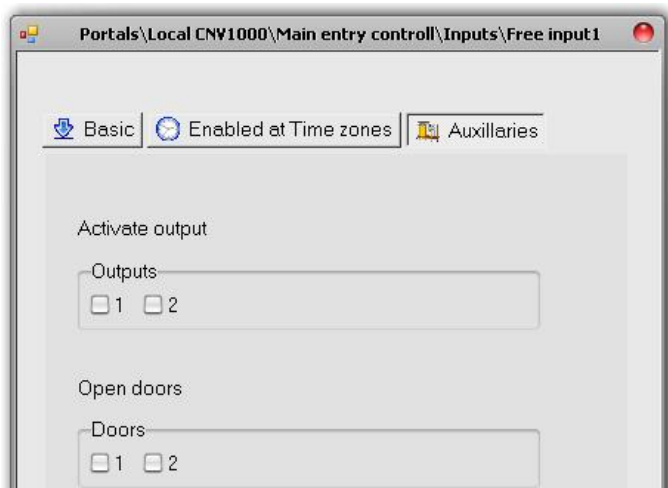
- Set the values in the Basic tab



- **Name:** Type Input Name
- **Type:** Select the normal state of the contact energizing the input (NO = no voltage on input, NC = input powered)
- **Enable:** Check to enable input
- **Enabled by Time zones:** Check if you need to enable time periods
- **Fire alarm:** Dedicate input to Fire alarm input
- If Enabled (Time zones are checked), set the time zones for which the input is enabled



- Set the Auxiliaries options



- **Activate outputs:** Outputs to be triggered on input activation
- **Open doors:** Doors to be released on input activation

- Click on the Save & Exit button
- Repeat the reader configuration procedure for the other inputs available on the same controller
- If the Automatic update for controllers option is set, PROS will configure the controller immediately, if it is not set, update the controller manually using the controller menu option "Send configuration"



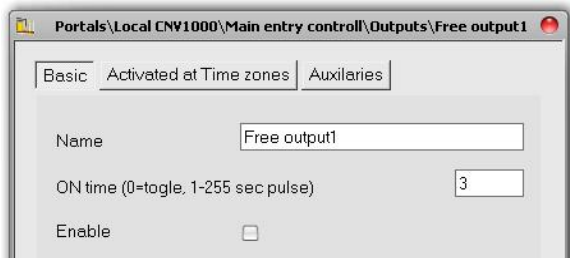
Outputs

Output configuration

- Right-click on the output to be configured and select the Properties item from the output drop-down menu



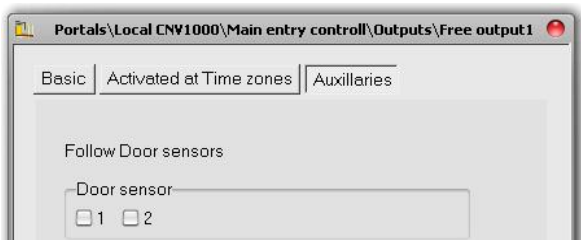
- Set the values in the Basic tab



- **Name:** Type the Output Name
- **ON time:** Select how long the output relay should stay energized. Enter 0 to toggle the relay state on event.
- **Enable:** Check to enable output
- Select the Activated at Time zones tab if you need to use the output as a time activated relay



- Click on the Auxiliaries tab to select if the output relay should follow the door state



- Click on the Save & Exit button
- Repeat the output configuration procedure on the other outputs available on the same controller
- If the Automatic update for controllers option is set, PROS will configure the controller immediately, if it is not set, update the controller manually using the controller menu option "Send configuration"



Output control

Right-click on the output to be controlled and select the control item from the drop-down menu



- **Enable:** Enables output
- **Disable:** Disables output
- **Activate:** Output responds as programmed to behave when it is ON

Access settings

Time zones

Time zones are time periods with validity defined by a start and stop time in a day, weekdays and holidays tag. The total number of time zones is 24. Planning the time zones should be done carefully, because the same zones are used for access levels, doors, readers, inputs and outputs configuration. It is recommended to plan this issue carefully before starting the system configuration.

- Double-click on the Time Zone item in the Users panel



- Fill in the time zones table

Time zones											
TZ	Time zone name	Begin	End	Hol	Mon	Tue	Wed	Thu	Fri	Sat	Sun
1	Work time	09:00	17:00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	Time Zone2	00:00	23:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- **Time zone name:** Enter the Time zone name
- **Begin:** Enter the time zone start time of the day
- **End:** Enter the time zone end time of the day
- **Hol:** Set if the time zone is valid for holidays
- **Mon-Sun:** Set the weekday's validity

- Click on the Save & Exit button
- If the Automatic update for controllers option is set, PROS will configure the controllers immediately, if it is not set, update each controller manually using the controller menu option "Send configuration"

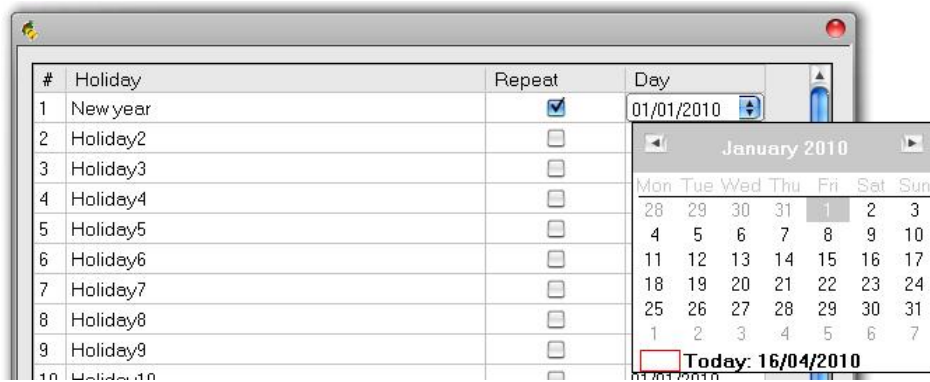


Holidays

- Double-click on the Holidays item in the Users Panel



- Enter the holidays



- **Holiday column:** Enter the holiday name

- **Repeat column:** Check to make the holiday valid annually

- **Day column:** Enter the holiday date or click on the right side and select the date in the new calendar window

- Click on the Save & Exit button
- If the Automatic update for controllers option is set, PROS will configure the controllers immediately, if it is not set, update each controller manually using the controller menu option "Send configuration"



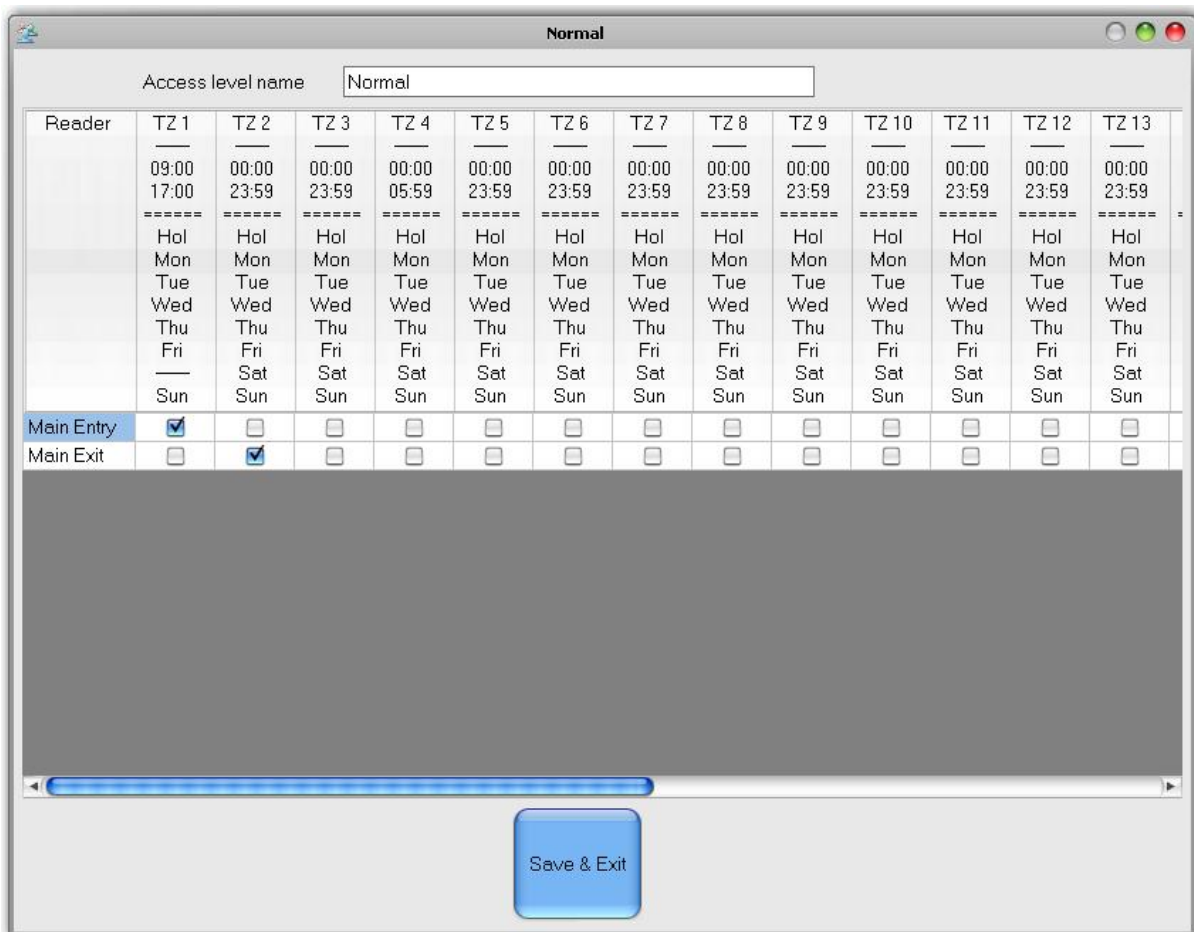
Access levels

Adding Access level

- Right-click on the Access level main item in the Users Panel and click on "Add new Access level"



- Enter the Access level name



Access level name:

Reader	TZ 1	TZ 2	TZ 3	TZ 4	TZ 5	TZ 6	TZ 7	TZ 8	TZ 9	TZ 10	TZ 11	TZ 12	TZ 13
	09:00 17:00	00:00 23:59	00:00 23:59	00:00 05:59	00:00 23:59	00:00 23:59	00:00 23:59	00:00 23:59	00:00 23:59	00:00 23:59	00:00 23:59	00:00 23:59	00:00 23:59
	Hol	Hol	Hol	Hol	Hol	Hol	Hol	Hol	Hol	Hol	Hol	Hol	Hol
	Mon	Mon	Mon	Mon	Mon	Mon	Mon	Mon	Mon	Mon	Mon	Mon	Mon
	Tue	Tue	Tue	Tue	Tue	Tue	Tue	Tue	Tue	Tue	Tue	Tue	Tue
	Wed	Wed	Wed	Wed	Wed	Wed	Wed	Wed	Wed	Wed	Wed	Wed	Wed
	Thu	Thu	Thu	Thu	Thu	Thu	Thu	Thu	Thu	Thu	Thu	Thu	Thu
	Fri	Fri	Fri	Fri	Fri	Fri	Fri	Fri	Fri	Fri	Fri	Fri	Fri
	Sun	Sat	Sat	Sat	Sat	Sat	Sat	Sat	Sat	Sat	Sat	Sat	Sat
Main Entry	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Main Exit	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Save & Exit

- Check the Allowed access time zones for each reader. Each column represents one time zone. The column headers display the time zone setting. For example, as shown in the picture above, the Access level is defined by authorization on the readers Main entry and Main exit in the first time zone (from 9:00 to 17:00 each day of the week and holidays).
- Click on the Save & Exit button
- If the Automatic update for the controllers option is set, PROS will configure the controllers immediately, if it is not set, update each controller manually using the controller menu option "Send configuration"



Edit access level

- Expand the access level item in the Users Panel, right-click on the Access level and select the "Properties" menu item



- Edit the Access level
- Click on the Save & Exit button
- If the Automatic update for controllers option is set, PROS will configure the controllers immediately, if it is not set, update each controller manually using the controller menu option "Send configuration"



Delete Access Level

- Expand the Access Level item in the Users Panel, right-click on the Access level and select the "Delete" menu item. The Access Level cannot be deleted if any users are assigned to it.



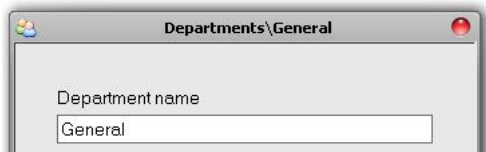
Departments

Add a Department

- Right-click on the Departments item in the Users Panel and click on "Add new"



- Enter the Department name and click on the save & Exit button



Edit a Department

- Expand the Department item in the Users Panel, right-click on the Department and select the "Edit" menu item



- Edit the Department name
- Click on the Save & Exit button

Delete a Department

- Expand the Department item in the Users Panel, right-click on the department and select the "Delete" menu item.



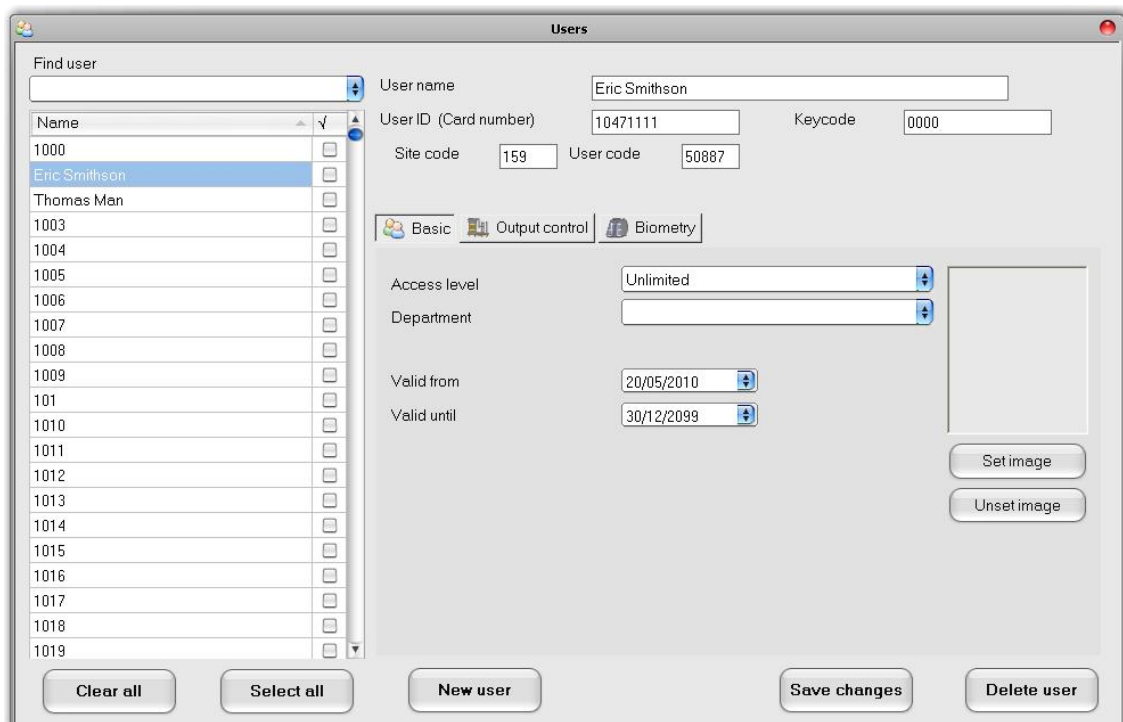
Users

Double-click on the Users item in the Users Panel to open the Users window

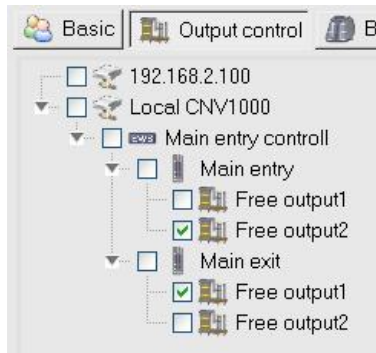


Add a user

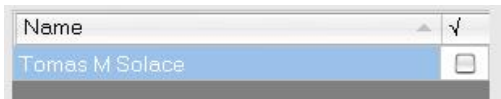
- Click on the New User button



- Enter the Name of the User
- Enter the User ID (card number). If there are two numbers on the card with values less than 65536 then use the Site code and the User code box.
- Select the Access level from the Access level drop-down list box
- Select the Department from the drop-down list box
- Select the from-until validity period
- Click on the Set image button and then browse for the User's image
- If the User should activate some outputs (not door relays), click on the Output control tab to select outputs



- Click on **Save**
- The entered User is added to the user table on the left side



- If the Automatic update for users option is set, PROS will upload the changes immediately, if it is not set, update each controller manually using the controller menu option Reload keys (Reload Users) after editing the users is completed and the users window is closed



Edit a user

- Select the User to be modified in the users table on the left side of the Users window



- Modify the user data (including the name if required)
- Click on the Save button
- If the Automatic update for users option is set, PROS will upload the changes immediately, if it is not set, update each controller manually using the controller menu option Reload (Reload Users) after editing the users is completed and the users window is closed

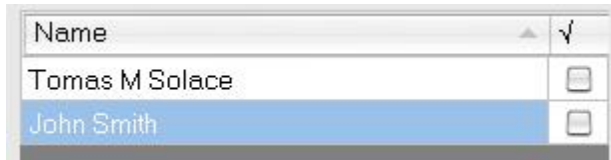


Delete a user

Warning!

Deleting a user erases the user from database. If you need to keep an activity record of the user, you can change the access level to "No access" instead of deleting the user, or generate the necessary reports and save them to a file (PDF is recommended), before deleting the user.

- Select the user to be deleted in the users table on the left side of the Users window



- Click on the Delete button
- If the Automatic update for users option is set, PROS will upload the changes immediately, if it is not set, update each controller manually using the controller menu option Reload keys (Reload Users) after editing the users is completed and the users window is closed



Fingerprints

Read me first

Selecting a finger for fingerprint enrollment

At least two fingerprints should be enrolled for each user in case of any abnormal situation like having an injured finger or carrying an object by hand.

In case of low recognition, the user can register the same fingerprint twice to increase the recognition rate. It is recommended to use the index or middle finger. If you choose another finger, the recognition rate may be decreased because it tends to be more difficult to place the finger in the center of the sensor area.

Caution while registering a fingerprint

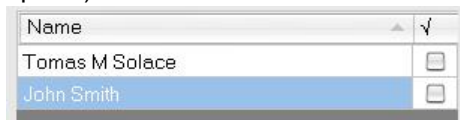
The initial fingerprint registration is important.

Because the recognition process compares the scanned fingerprint with the registered one, an abnormally registered fingerprint can cause a failure.

1. Put the center of your fingerprint on the middle of the sensor
2. If you have a cut on your finger or your fingerprint is not clear enough, retry with another finger
3. When the fingerprint recognition is in progress, do not move your fingerprint

Enrolling Fingerprints from a reader

- Select the User in the User Column, NOT the Check Box (the Check Box is used for sending the fingerprints) and the User Name cell will turn blue.



- Select the Fingerprint reader from where the enrollment will be done.



- Right click on the fingertip and select "Enroll".



- In the next 15 sec. present the finger on the selected reader and the finger tip will turn blue, with the percentage of successful enrollment shown next to the fingertip.



- Repeat the procedure for the other fingers (as required)
- Click on "Save templates". All the enrolled fingers will change their color to red.



Note: If more fingerprints are added for one user, all fingers will send the same Wiegand Code to the controller.

Enrollment from a desktop Reader

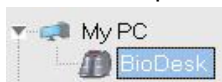
Install the Desktop Reader (BioE) using the drivers located on the CD provided with the Fingerprint Reader. It

is installed in the same way as a USB Device. When the desktop reader has been installed it will automatically appear in the Software.

- Select the User in the User Column, NOT the Check Box (the Check Box is used for sending the fingerprints) and the User Name cell will turn blue.



- Select the desktop reader from where the enrollment will be done.



- Right click on the fingertip and select "Enroll".



- In the next 15 sec. present the finger on the selected reader and the finger tip will turn blue, with the percentage of successful enrollment shown next to the fingertip.



- Repeat the procedure for the other fingers (if needed)
- Click on "Save templates". All the enrolled fingers will change color to red.

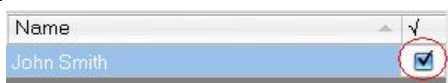


Note: If more fingerprints are added for one user, all fingers will send the same Wiegand Code to the controller.

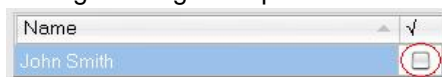
1. First the reader must be selected from where the enrollment will be done. In this case, we select the Desktop reader.
2. Right click on the fingertip and select "Enroll".
3. In the next 15 sec. present the finger on the reader (the desktop reader) and the finger tip will turn blue, with the percentage of successful enrollment shown next to the fingertip.
4. Click on "Save templates".

Uploading the fingerprints to the Fingerprint readers

- Select the Users whose fingers templates will be sent to the reader, by clicking on the checkbox of the user



- Select the Fingerprint Reader to where the Users data should be sent and click on "Upload selected users to reader"
- As each user is being sent, the checkbox will uncheck indicating that the user has been successfully sent. At the same time the Amber LED of the Fingerprint Reader will blink. Note: The average time for transferring one finger template is 0.8 sec.



Note: If there were any PIN Codes available, they will also have been sent.

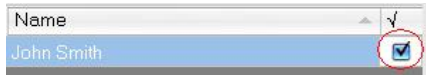
Deleting Fingerprints

In General, after transferring, the fingerprints are stored in the Fingerprint Reader and in the Software.

Deleting can be done only in the software, only in the readers or from both places.

Deleting one user from the fingerprint Reader

- Select the user's checkbox



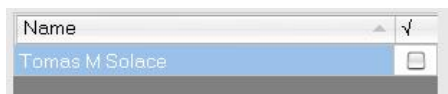
- Select the Reader from where the users should be deleted and click on "Delete selected users from selected readers". The user is then deleted from the reader, but the fingerprints remain in the software's database. They can be sent once again without the need of re-enrollment.

Deleting all users from the fingerprint Reader

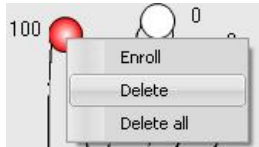
- Select the Reader from where the users should be deleted and click "Erase Reader Database".

Deleting user finger templates from the Software

- Select the User.



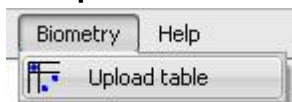
- Go to the fingertip that needs to be deleted, right click and select "Delete" for one finger or "Delete All" for all fingers of the User. With this procedure the User's fingerprints are deleted from the software, but they remain present in the reader.



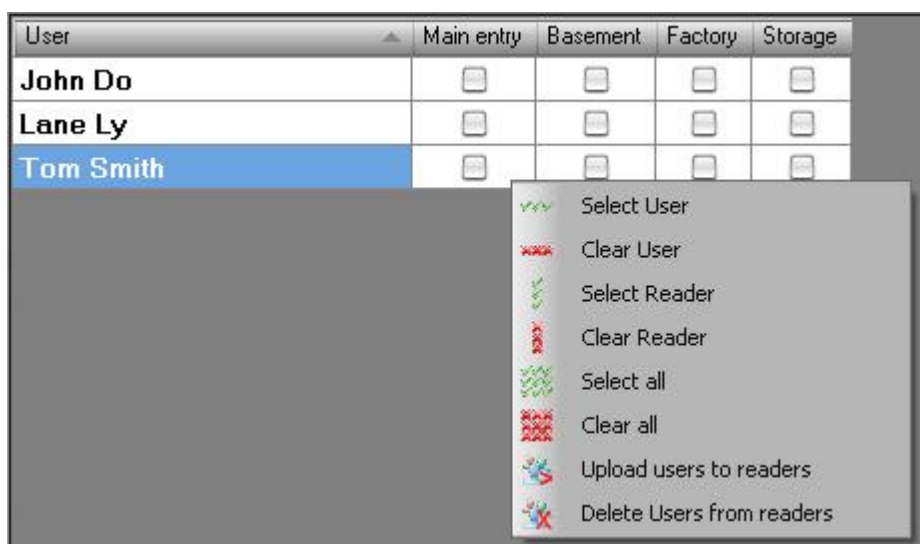
Complex upload

Complex user upload is used to send multiple user selections to many readers.

- Click on **Upload table** in the main menu



- Use the mouse click to select the combination you need or use right-click to check or clear an entire row or column



- Select **Upload Users to readers** or **Delete Users from readers** in the right-click menu
- As the upload progresses, the check boxes are cleared showing that the appropriate combination was successfully done
- When the upload is completed, if there are still some checked items, repeat the upload command

Reports

To generate reports expand the Reports item in the User panel.



All reports are shown on the report form with following buttons:



Export - save report to disk or send it to mail recipient in various file formats (PDF, Excel, Text...)



Print - print report



Navigation - to view the First page, Previous page, Next page, Last page



Refresh - refresh data on the report



Find - search for specific text in the report



Zoom - change the zoom factor of the displayed report, does not affect exported or printed report

User list report

- Double-click on the ID item in the expanded Reports item
- Wait for the report to be generated as shown

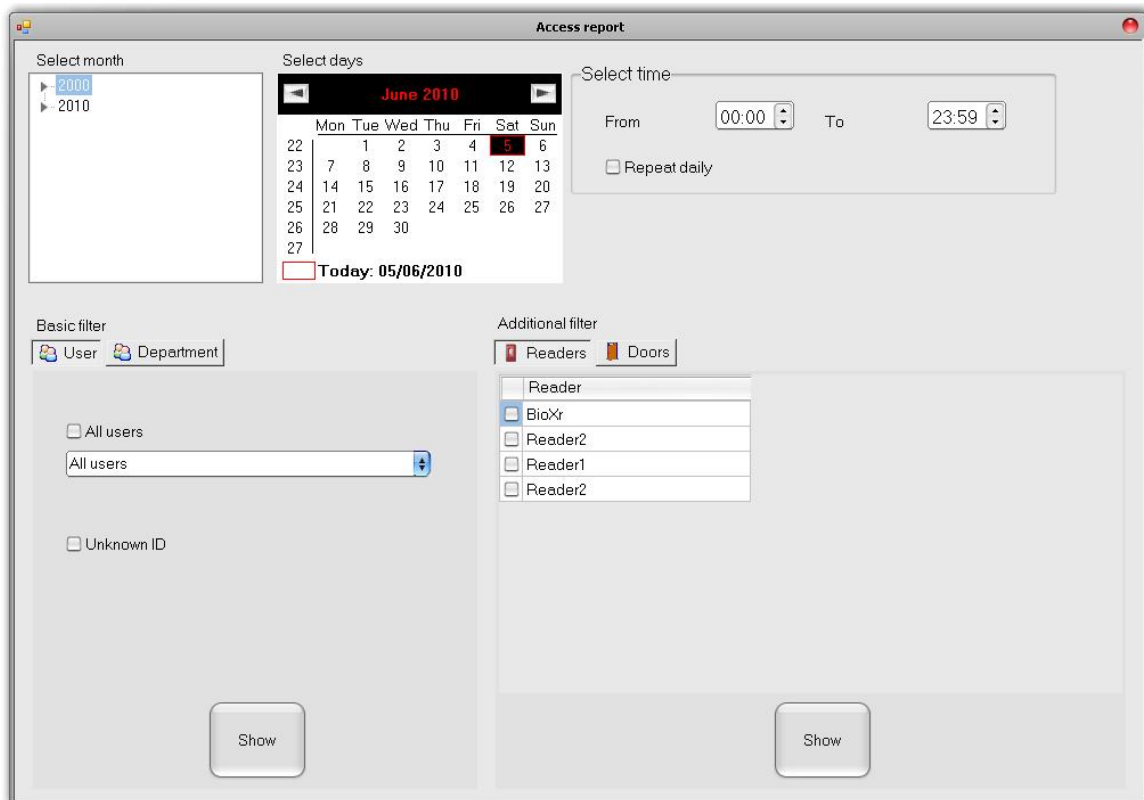
ID list

User	ID
John Smith	456456

Access reports

Load report window

- Double-click on the Access item in the expanded Reports item to open the Access report window

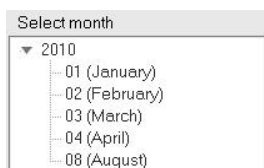


The screenshot shows the 'Access report' window with the following sections:

- Select month:** A tree view showing '2000' and '2010'.
- Select days:** A calendar for June 2010. The date 05/06/2010 is selected. Below the calendar, it says 'Today: 05/06/2010'.
- Select time:** Two time pickers for 'From' (00:00) and 'To' (23:59). There is a checkbox for 'Repeat daily'.
- Basic filter:** Two tabs: 'User' and 'Department'. Under 'User', there is a checkbox for 'All users' and a text box containing 'All users'. There is also a checkbox for 'Unknown ID'.
- Additional filter:** Two tabs: 'Readers' and 'Doors'. Under 'Readers', there is a list box containing 'Reader', 'BioXr', 'Reader2', 'Reader1', and 'Reader2'.
- Show buttons:** Two 'Show' buttons at the bottom of the Basic filter and Additional filter sections.

Set time filters

- Expand the month window and click on the desired month



The screenshot shows the 'Select month' window with a tree view. The year '2010' is expanded, showing a list of months: '01 (January)', '02 (February)', '03 (March)', '04 (April)', and '08 (August)'.

*Only the months with events are shown in the month window

- Select days

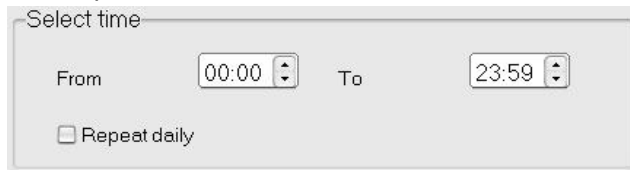


The screenshot shows the 'Select days' window with a calendar for April 2010. The date 20/04/2010 is selected. Below the calendar, it says 'Today: 20/04/2010'.

- For a one-day report click on the selected day in the month calendar.

- For a range of days click and hold the left mouse button on the first day of the range, drag to the last day of the range and release the mouse.

- Select time period



Select time

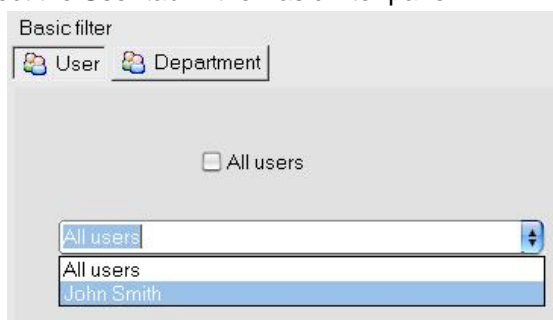
From To

☐ Repeat daily

- If Repeat daily is checked, reports will be generated for the selected time range of the day, every day in the selected days range

User report

- Set time filters
- Select the User tab in the Basic filter panel



Basic filter

☒ User ☐ Department

☐ All users

All users
John Smith

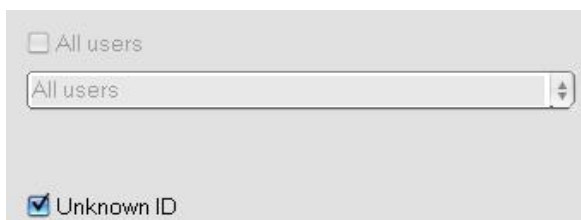
- Select the user name from the drop-down list box
- For a report of all users, check the "All users" item
- Click on the Show button at the bottom of the Basic filter panel to load the report

User report: John Smith

06 April 2010 00:00 - 27 April 2010 23:59		
Time	Reader	Event
Monday 19 April 2010		
02:26.10	Main entry	Access granted

Unknown ID report

- Set time filters
- Select the User tab in the Basic filter panel
- Check "Unknown ID"



☐ All users

☒ Unknown ID

- Click on the Show button at the bottom of Basic filter panel to load the report

Unknown ID Report

01 June 2010 00:00 - 05 June 2010 23:59

Time	ID	Reader	Event
Tuesday 01 June 2010			
21:59.18	456456	Main Entry	Access denied = ID unknown
22:06.03	456456	Main Entry	Access denied = ID unknown
22:52.15	456456	Main Entry	Access denied = ID unknown

Department report

- Set time filters
- Select the Department tab in the Basic filter panel



- Select the department from the drop-down list box
- Click on the Show button at the bottom of Basic filter panel to load the report

Department report: General

06 April 2010 00:00 - 20 April 2010 23:59

Time	User	Event	Reader
Monday 19 April 2010			
02:26.10	John Smith	Access granted	Main entry

Adding a reader filter to Access report

- Set time filters
- Set filter for User or Department report
- Select the Readers in the additional filter panel



- Click on the Show button at the bottom of Additional filter panel to load the report

All users report

06 April 2010 00:00 - 20 April 2010 23:59

At readers: Main entry

Time	User	Reader	Event
Monday 19 April 2010			
02:26.10	John Smith	Main entry	Access granted

Adding a Doors filter to Access report

- Set time filters

- Set the filter for User or Department report
- Select the Doors in the additional filter panel

Additional filter

☒ Readers ☒ Doors

☐ Door

☒ Main door

☐ Door2

- Click on the Show button at the bottom of the Additional filter panel to load the report

User report: John Smith

06 April 2010 00:00 - 20 April 2010 23:59

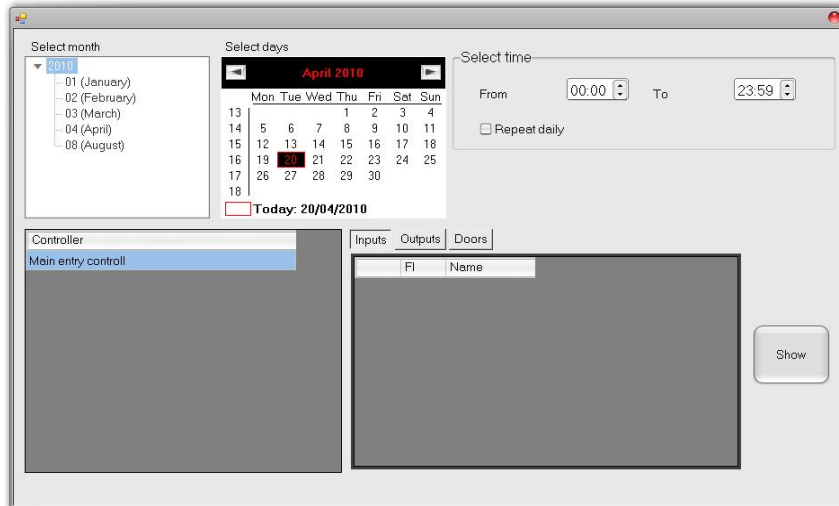
At doors: Main door

Time	Reader	Event
Monday 19 April 2010		
02:26:10	Main entry	Access granted

I/O reports

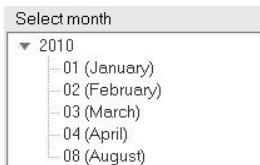
Load report window

- Double-click on the Access item in the expanded Reports item to open the IO report window



Set time and controllers filters

- Expand the month window and click on the desired month



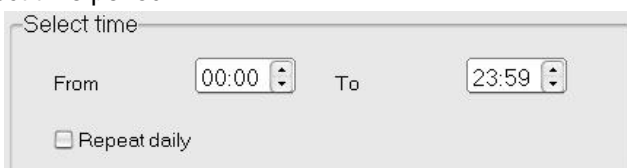
*Only the months with events are shown in the month window

- Select days



- For a one-day report click on the selected day in the month calendar.
- For a range of days click and hold the left mouse button on the first day of the range, drag to the last day of the range and release the mouse.

- Select time period



- If Repeat daily is checked, reports will be generated for the selected time range of the day, every

day in the selected days range

- Select controller in the Controller table

Controller
Main entry controll

Inputs report

- Set time and controller filters
- Select the Inputs in the additional filter panel

Inputs	Outputs	Doors
<input checked="" type="checkbox"/>	FI	Name
<input checked="" type="checkbox"/>	1	Free input1
<input type="checkbox"/>	2	Free input2

- Click on the Show button load report

Outputs report

- Set time and controller filters
- Select the outputs in the additional filter panel

Inputs	Outputs	Doors
<input type="checkbox"/>	FO	Name
<input checked="" type="checkbox"/>	1	Free output1
<input checked="" type="checkbox"/>	2	Free output2

- Click on the Show button load report

Doors report

- Set time and controller filters
- Select the Doors in the additional filter panel

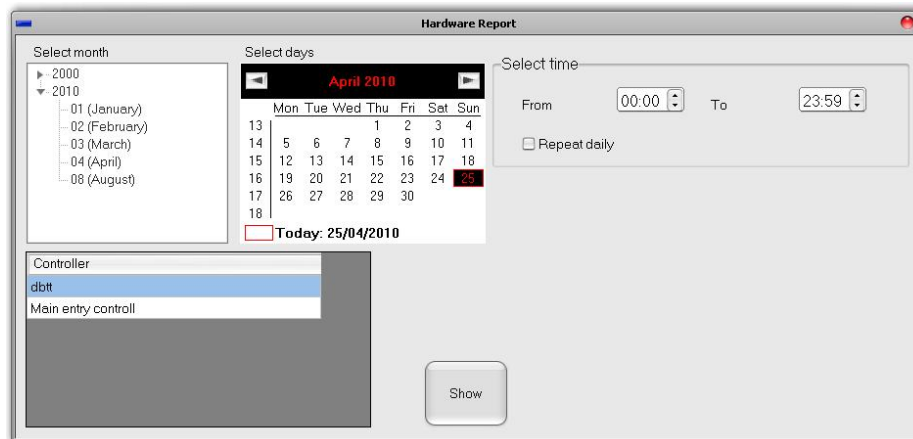
Inputs	Outputs	Doors
<input type="checkbox"/>	<input type="checkbox"/>	Door
<input checked="" type="checkbox"/>	<input type="checkbox"/>	1
<input type="checkbox"/>	<input type="checkbox"/>	2
<input type="checkbox"/>	<input type="checkbox"/>	Main door
<input type="checkbox"/>	<input type="checkbox"/>	Door2

- Click on the Show button load report

HardwareReport

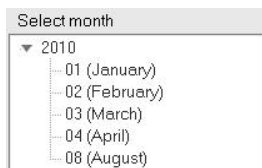
Load report window

- Double-click on the Access item in the expanded Reports item to open the Hardware report window



Set time and controllers filters

- Expand the month window and click on the desired month



*Only the months with events are shown in the month window

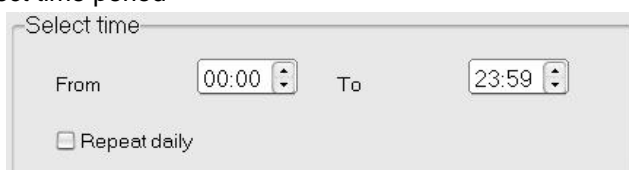
- Select days



- For a one-day report click on the selected day in the month calendar.

- For a range of days click and hold the left mouse button on the first day of the range, drag to the last day of the range and release mouse.

- Select time period



- If Repeat daily is checked, reports will be generated for the selected time range of the day, every day in the selected days range

- Select controller in the Controller table



- Click on the Show button load report

Controller Main entry controll - Hardware report

01 April 2010 00:00 - 30 April 2010 23:59

Time	Controller	Event	Reader
04/04/2010			
2:33:00	Main entry controll	Power Loss	
11/04/2010			
19:40:08	Main entry controll	System ON	

Program operators

Add an operator

- Right-click on the Operators menu in the User panel and select Add operator



- In the Operator window enter the Name, Password and select the operator's options



- Click on the Add & Exit button

Edit an operator

- Right-click on operator and select Properties menu



- Edit the operator properties in the operator window and click on the Add & Exit button

Delete an operator

- Right-click on the operator and select the Delete menu



Troubleshooting

- **EWSi portal (CNV-1000) is not found in "Search network portals"**

1. Check if EWSi is powered
2. Check if EWSi and the PC are connected to the network
3. Disable the network firewall
4. Check the port value in the search window

- **EWSi portal (CNV-1000) is found, but can't be configured**

1. Check if the password in the search window matches the EWSi password. If you forget the password, use the reset button in the EWSi to set the CNV-1000 to default values.
2. Check the port value in the search window
3. If the PC IP address has a different IP network, set it to the same network, configure the router and restore the PC settings to the previous value.

Example:

- If the PC IP address is 10.10.10.5 and the EWSi IP address is 192.168.1.100, set the PC IP to value 192.168.1.X where X is between 1 and 254, taking care not to set the same address as the EWSi or another existing IP address in the network
- Configure EWSi
- Set the PC IP address back to 10.10.10.5

- **EWS does not react on reader reading (Reader's LED stays inactive)**

1. EWS Wiegand is not set to match the reader
2. Check the reader power supply
3. Replace the reader

- **Devices connected to the USB to RS485 converter are offline**

1. The USB converter is represented as a COM Port on the PC side. If the converter is plugged into another USB port, the COM number will be changed. The solution is to plug the converter into the initial USB port or to change the COM value in the Portal properties.
2. Check the converter connections

- **Controllers change connection state (controller icon changes background color to red)**

1. If the controller is using an RS485 connection, check for cable damage, termination load (120 Ohm) and quality of cables
2. More than 31 units, the controllers and readers are connected to the same RS485 bus

- **Cannot get events report for User**

1. The user was deleted and entered again with the same name. Once the user is deleted, all events for the user are deleted. Entering a new user with same name will not retrieve the events. The solution is not to delete the user (you can change the access level to "Nowhere" instead) or generate reports for the user and export them to a PDF, Excel or Text file for keeping.

Biometry

- **Reader reading performance is decreased**

1. Check if the fingerprint reading area is dirty. Do not clean the device with any form of liquid. Use a soft and dry cloth only.
2. The reading area is damaged. If the damage is minor, try to [calibrate the sensor](#)

- **Fingerprint is not recognized normally**

1. If your finger is wet, retry after drying it.
2. When your finger is too dry, retry after blowing on your fingertip.
3. If you have a cut on your registered finger, register another fingerprint.

- **Fingerprint is recognized, but EWS reports another ID number**

1. If the user is not deleted from the reader and the user is enrolled again with a new ID, the reader will recognize the finger with the first ID. To resolve this, delete all users from the reader and re-upload all users to the reader.

Glossary

A

Access Area: A restricted access area controlled by a reader. One area can contain other separate areas, such as one or a group of rooms, parking lot, fenced restricted area...

Access controller: When a credential is presented to a reader, the reader sends the credential's information, usually a number, to a Control panel, a highly reliable processor. The control panel compares the credential's number to an internal access control list, grants or denies the presented request, and sends a transaction log to a database. When access is denied based on the access control list, the door remains locked. If there is a match between the credential and the access control list, the control panel operates a relay that in turn unlocks the door. The control panel also ignores a door open signal to prevent an alarm. Often the reader provides feedback, such as a red LED for access denied and a green LED for access granted. Smart electronics with the ability to remember the User's ID; Time zones; Events; to control Doors; Relays; to receive information about the Door state; Inputs; Readers; to communicate with Access control software and to take action based on events and programmed parameters

Access level: Definition of time zones for each reader. Users can access readers only during the defined time zones in the Access level to which they belong. One user can be assigned to one Access level only. The same time zone can be used in an unlimited number of Access levels.

Anti-passback: Prevention of allowing the user to enter an area more than once with the same ID. It prevents users lending their ID to another person for the purpose of entering the area. This function is useful when a higher level of security is needed, counting the number of persons in areas, time attendance, fire reports, etc. Anti-passback can have more variations. It can be valid for one or more readers, one or more doors, can be reset at a fixed time of the day, can prevent double access within a given period of time. Since the Access controller is enforcing these restrictions, Anti-passback can be enforced only on doors and readers connected to the same controller.

B

Biometry: The way of recognizing specific body parts specific to each person. The most common parts used in security systems are Fingerprint, Face, Eye, Finger vein, Voice and Palm. For higher security, biometry can be mixed and combined with standard access techniques like Fingerprint + Proximity card, Fingerprint + Code.

C

Code: Personal identification presented by typing a sequence of numbers on a keypad. Depending on the keypad model it can be with a fixed or variable length.

COM, COM port: Serial communication interface. Can be an existing PC port or can be an external component. The external component can be a USB device with drivers or a network device using drivers on the PC side to create a virtual COM port.

Control panel: Same as Access controller

D

Department: Grouping the users by internal organization. Used for printing reports with a convenient grouping of users.

Door contact sensor: The sensors are standard magnetic door sensors used in security applications. Either Normally Open or Normally Closed Sensors can be used. Normally Closed sensors (door closed, switch closed) are recommended so that an alarm can be generated if the connection wire breaks.

E

Egress button, Exit switch: Push-button used to open the door from the protected area side. It is connected to the Access controller. Electronic touch sensors can be used with the same function.

Electric strike: An access control device used for doors. It replaces the fixed strike faceplate often used with a latchbar (also known as a *keeper*). Like a fixed strike, it normally presents a ramped surface to the locking latch allowing the door to close and latch just like a fixed strike would. However, an electric strike's ramped

surface can, upon command, pivot out of the way of the latch allowing the door to be pushed open (from the outside) without the latch being retracted (that is, without any operation of the knob) or while exited the knob or lever can be turned to allow egress from the secured area.

Electric strikes generally come in two basic configurations:

- **Fail-secure.** Also called Fail-locked or non-fail safe. In this configuration, applying electrical current to the strike will cause it to open. In this configuration, the strike would remain locked in the event of a power failure, but typically the knob can still be used to open the door from the inside for egress from the secure side. These units can be powered by AC which will cause the unit to "buzz", or DC power which will offer silent operation, except for a "click" while the unit releases.
- **Fail-safe.** Also called Fail-open. In this configuration, applying electrical current to the strike will cause it to lock. In this configuration, it operates the same as a magnetic lock would. If there is a power failure, the door would open merely by being pushed/pulled open. Fail safe units are always run using DC power.

F

Fingerprint reader: Reader with the ability to recognize a human finger and send information to the Access controller.

Fire alarm input: Triggering this input will release all doors controlled by the Control panel

Firmware: Programs and data structures that internally control various electronic devices

Free Input: Additional inputs available in the Access controller. Not dedicated to the primary role of Access control. Can be configured for additional monitoring of other events (Alarm, Fire...) or user action (Bell, Panic...)

Free output: Additional outputs available in the Access controller. Not dedicated to primary role of Access control. Can be configured for the execution of some tasks (Timer, Alarm bell, Light control...).

I

ID: Identification number presented to the Access controller by the Reader. The reader gets information from the media presented (Proximity card, Code, Biometry) and translates it to a number format that the Access controller can recognize.

Input: A hardware gate on the Access controller able to receive information about other equipment. It can be dedicated to a specific task (door monitor, egress button...) or can be programmatically assigned to monitor other devices (Intruder alarm, fire, temperature). The access controller can be programmed to execute specific actions following the change of the inputs state. Inputs can only have two states (OFF/ON). Inputs are also used to pass the information to the Access control software.

IP Address: The **Internet Protocol (IP) address** is a numerical label that is assigned to devices participating in a computer network that uses the Internet Protocol for communication between its nodes.

IP Port: The port number is a 16-bit unsigned integer, ranging from 0 to 65535. The process associates with a particular port (known as *binding*) to send and receive data, meaning that it will listen for incoming packets whose destination port number and IP destination address match that port, and/or send outgoing packets whose source port number is set to that port.

M

Magnetic lock: A simple locking device that consists of an electromagnet and armature plate. By attaching the electromagnet to the door frame and the armature plate to the door, a current passing through the electromagnet attracts the armature plate holding the door shut.

Mantrap: A group of doors with the logic that only one door can be open at a time. Opening one of the doors leads to the locking of all other doors until the closure of the first one. Using a combination of inputs and outputs, a mantrap can be extended to doors from different Access controllers in the same site.

O

Operator: A person listed in the Access control software with given rights for one or more options.

P

Portal: A hardware interface between the Access control software and the devices installed in the system. One portal can connect one or more devices to the software. A portal can exist as a single device or as part of the Access controller.

R

Reader: A device installed near the access barrier (door, gate, turnstile..) to recognize user identification media (card, code, finger..) and to send information to the Access controller.

Relay: An electrical component used as an output by the Access controller. It provides electric isolation between the Access controller and the device that is controlled by the output. The relay has two states: ON and OFF. The output of the relay provides a mechanical switch contact with two outputs - one contact is open when the relay is energized and the other is closed.

T

Time zone: The definition of the time period of the day used to later define system behavior by time periods. The time zone also has weekday and holiday definitions as additional filters for system behavior.

Touch sensor: An electronic device that reacts to human touch. Mostly used as an egress button.

W

Wiegand interface: A wiring standard used to connect a card swipe mechanism to the rest of the electronic entry system. A Wiegand-compatible reader is normally connected to a Wiegand-compatible security panel.